NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RAPIDLY DEPLOYABLE, SELF FORMING, WIRELESS NETWORKS FOR MARITIME INTERDICTION OPERATIONS

by

Georgios Stavroulakis

September 2006

Thesis Advisor:	Alex Bordetsky
Second Reader:	Eugene Bourakov

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Rapidly Deployable, Self Forming, Wireless Networks for Maritime Interdiction Operations.			**5. FUNDING NUMBERS**
6. AUTHOR Georgios Stavroulakis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The term "Maritime Interdiction Operations" usually refers to Visit, Board, Search and Seizure (VBSS) operations executed today all over the world. These operations are conducted as a part of the maritime law enforcement policy of each country inside their respective territorial waters or as a part of the homeland security requirements as they are mandated today by the global war against terrorism. Very often lately, they are conducted by allied maritime forces in international waters as well.

Although such operations might seem quite simple in execution, the global war against terrorism has dramatically increased their level of complexity. In the past, searching cargo ships for illegal or contraband cargo was not that complicated or that important for national security, but now, searching for non-proliferation, radiological or bio-chemical material, as well as for possible terrorists among the crew members of a ship, is a very complex operation that cannot tolerate mistakes or omissions.

This thesis examines the requirements posed by a boarding team, either from the navy or the law enforcement community, on information flow from and to them, in order to enhance their situational awareness and decision making capability during Maritime Interdiction Operations. That information flow is provided by several wireless network technologies, implemented during field trials, as part of the NPS CENETIX (Center for Network Innovation and Experimentation) lab's maritime subset of experimentation. During these field trials, a wireless extension of the internet is deployed to the sea, allowing the boarding team to access information and collaborate with remotely located experts and respective operational commands; the technical aspects, the benefits and shortcomings of the utilized technologies and collaborative tools are screened against the maritime war fighter's operational requirements.

14. SUBJECT TERMS Maritime Interdiction Operations, Boarding Party, IEEE 802.16, Mesh, Self Healing, Rapidly Deployable, Wireless Networks, Ultra Wideband (UWB) Technology, Operational Requirements, Tactical Network Topology (TNT)	**15. NUMBER OF PAGES** 103
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RAPIDLY DEPLOYABLE, SELF FORMING, WIRELESS NETWORKS FOR MARITIME INTERDICTION OPERATIONS

Georgios Stavroulakis
Lieutenant Commander, Hellenic Navy
B.S., Hellenic Naval Academy, 1991

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Georgios Stavroulakis

Approved by: Alex Bordetsky
Thesis Advisor

Eugene Bourakov
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The term “Maritime Interdiction Operations” usually refers to Visit, Board, Search and Seizure (VBSS) operations executed today all over the world. These operations are conducted as a part of the maritime law enforcement policy of each country inside their respective territorial waters or as a part of the homeland security requirements as they are mandated today by the global war against terrorism. Very often lately, they are conducted by allied maritime forces in international waters as well.

Although such operations might seem quite simple in execution, the global war against terrorism has dramatically increased their level of complexity. In the past, searching cargo ships for illegal or contraband cargo was not that complicated or that important for national security, but now, searching for non-proliferation, radiological or bio-chemical material, as well as for possible terrorists among the crew members of a ship, is a very complex operation that cannot tolerate mistakes or omissions.

This thesis examines the requirements posed by a boarding team, either from the navy or the law enforcement community, on information flow from and to them, in order to enhance their situational awareness and decision making capability during Maritime Interdiction Operations. That information flow is provided by several wireless network technologies, implemented during field trials, as part of the NPS CENETIX (Center for Network Innovation and Experimentation) lab’s maritime subset of experimentation. During these field trials, a wireless extension of the internet is deployed to the sea, allowing the boarding team to access information and collaborate with remotely located experts and respective operational commands; the technical aspects, the benefits and shortcomings of the utilized technologies and collaborative tools are screened against the maritime war fighter’s operational requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

ADC	Analog to digital converter
AN-50e	Redline Communications' system
AN-80	Redline Communications' system
AP	Access Point
BOD	Bandwidth on demand
BPSK	Binary Phase Shift Keying
BS	Base station
CENETIX	Center for Network Innovation and Experimentation
CSMA/CA	Carrier sense multiple access/collision avoidance
dB	Decibel
dBm	db referenced to 1 mW
DCF	Distributed coordination function
DEA	Drug Enforcement Administration
DL	Down link
DMT	Discrete multi-tone
DoD	Department of Defense
DOE RAP	Department of Energy Radiological Assistance Program
EIRP	Effective Isotropic Radiated Power
EMI	Electromagnetic Interference
EOD	Explosives ordnance disposal
FCC	Federal Communications Commission
FDM	Frequency division multiplexing
FLASH OFDM	Fast, Low-Latency Access with Seamless Handoff Orthogonal Frequency Division Multiplexing
FMDM	Flarion's Mobile Diagnostic Monitor
Gbps	Gigabits per second
GIG	Global Information Grid
GHz	Gigahertz

GPS	Global Positioning System
HVT	High Value Target
ICMP	Internet control message protocol
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISI	Inter-symbol interference
JAC	Joint Analysis Center
Km	kilometers
LAN	Local Area Network
LLNL	Lawrence Livermore National Laboratory
LOS	Line of Sight
LPI/D	Low probability of Intercept and Detection
MAC	Media Access Control
Mbps	Megabits per second
MBWA	Mobile Broadband Wireless Access
MCM	Multi-carrier modulation
MCM	Mine counter measure
MHz	Megahertz
MIB	Management Information Base
MIFC	Maritime Intelligence Fusion Center
MIO	Maritime Interdiction Operation
MOUT	Military Operations in Urban Terrain
MSST	Maritime Safety and Security Team
MTBF	Mean Time Between Failures
NATO	North Atlantic Treaty Organization
NBFC	National Biometrics Fusion Center
NCW	Network centric warfare
NLOS	Non-line of sight
nm	nautical miles

OFDM	Orthogonal Frequency Division Multiplexing
PCI	Peripheral Component Interconnect
PG	Processing Gain
PMP	Point-to-Multipoint
PSD	power spectral density
PtP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RF	Radio Frequency
RHIB	Rigid hull inflatable boat
Ro-Ro	Roll on/roll off
RSSI	Received Signal Strength Indicator
Rx	receiver
SA	Situational Awareness
SC	sub-carrier
SFPD	San Francisco Police Department
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SOCOM	Special Operations Command
SOP	Standard operating procedures
SS	Subscriber station
TDMA	Time division multiple access
TNT	Tactical Network Topology
TOC	Tactical Operations Center
Tx	transmitter
UAV	Unmanned Aerial Vehicle
UHF	Ultra high frequency
UN	United Nations
USCG	United States Coast Guard
UWB	Ultra wide band

VHF	Very high frequency
W	Watt
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WLL	Wireless local loop
WMAN	Wireless Metropolitan Area network
WMD	Weapons of mass destruction
WPAN	Wireless Personal Area Networks
XML	Extensible markup language

ACKNOWLEDGMENTS

I would like to express my deepest thanks to my thesis advisor Dr. Alex Bordetsky, and my second reader, Mr. Eugene Bourakov for giving me the opportunity to be a part of the CENETIX lab team. I appreciate their guidance and assistance in my thesis work, but most of all I appreciate their efforts in making the CENETIX lab a fun place to work in.

Above all, I must thank the two loves of my life, my wife Katerina and my daughter Olga for their support, love and understanding during my studies at NPS.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

All countries with a coastline have executed, for one reason or another, their right for boarding and inspecting vessels inside their territorial waters. Even in international waters, there are numerous examples of boarding operations that were conducted by allied forces in the past or are still running, in accordance with UN Security Council Resolutions and Sanctions or NATO's Article 5: the embargo on Iraq during the Desert Storm / Desert Shield operations in 1990-91, Operation Sharp Guard in the south Adriatic Sea between 1993 and 1996, the maritime part of Operation Enduring Freedom in the south Arabian Sea and Operation Active Endeavour in the Mediterranean since 2001.

There is a great variety of ways for conducting such operations: the boarding party can be shore-based or can be launched from a supporting vessel; a RHIB (Rigid Hull Inflatable Boat) or a helicopter can be utilized in order to transport the boarding team to the inspected vessel, and the inspected vessel may or may not comply with the boarding operation; in the latter case, prior to the actual search operation, an offensive operation must precede in order to seize and control the target vessel.

Among the different sorts of operational implementations, what is common in all boarding cases, is that the boarding team does not always have the necessary expertise, information and communication equipment to maintain situational awareness during these operations; in other words they do not have the capability to make the decisions they are required to. They usually stand alone on the target vessel, with the only connection to the outside world being a voice UHF or VHF radio transceiver that links them to shore or to the support vessel. This link does not match though, the information flow needs as they are dictated by the very nature of the boarding operation. The boarding party members, either from the law enforcement or the military community, no matter how well trained they might be, are no experts in correctly evaluating all their findings on board the inspected vessel and they have no means of verifying the authenticity of the ship's documentation or its crew members' identities. Therefore, a lot of data must be processed "externally" to the boarding team and thus, there is need for

transmitting that data timely and reliably. For example, the ship's crew and cargo manifests have to be scanned and transmitted to shore for verification, while, on many occasions, the crew's biometrics data and photographs also have to be sent to shore-based government organizations for cross referencing with their databases. Furthermore, there is need for transmission of video stream and photos of the ship's inner hull and machinery as well as radiation files obtained from radiation detection devices. All of the aforementioned procedures also need to be executed timely; sending the data and receiving the answers should not last more than the average time required to search a vessel. The boarding team might have to perform another boarding soon, while the searched vessel cannot be detained for long without reasonable evidence.

The standard boarding operating procedures at the moment do not provide any timeliness at all; all the gathered data has to be relayed sequentially through many different channels of communications, in the form of standardized text or voice messages, or even has to be physically delivered to the applicable recipients. Consequently, the boarding officer and the operational authority controlling the boarding operation, very often have to make decisions without having the right inputs. In absence of reliable and timely information, it is not uncommon for a vessel to be boarded, searched and released as "clean", only to later discover, when all the obtained pieces of data have been processed, that it should have been detained. In other words, traditional boarding operating procedures might be able to eventually provide situational awareness but when it is already too late to take the right decisions and assume the right actions.

B. OBJECTIVES

The feasibility of establishing ship-to-shore and ship-to-ship wireless links under certain conditions, has already been proven (Marvin, 2005), as well as the feasibility of stretching the link on the deck or inside the hull of the inspected vessel, during the TNT 05-3, 05-4, 06-1 field experiments. The next step and primary objective of this study is to examine:

- The performance of the utilized wireless technologies under more realistic scenarios, which more closely depict all possible aspects of a boarding operation.

- The operational requirements from such networks, as they are set by a boarding team, in order for those networks to provide accurate and timely situational awareness to the operators.
- The network behavior patterns in order to optimize the network performance, discover the best network setup and configuration, and match the operational requirements that are set by the boarding party.

C. RESEARCH TASKS

1. Operational Requirements Research Tasks

What characteristics should the utilized networking equipment have in order to match all the needs of the operators, under all possible realistic boarding scenarios?

2. Collaboration Research Tasks

Which should be the nodes of a MIO network, i.e., who should be included in the collaborative environment?

What kind of remotely located experts would a boarding officer like to have "virtually" included in the boarding party?

What kind of data is going to be shared through that kind of network, i.e., what would be the type, volume and frequency for exchanging files and messaging?

What types of collaboration would be the most appropriate for such operations?

How is that data going to enhance the situational awareness of the boarding officer, as well as of the operational command?

3. Network Performance Research Tasks

Which are the required network characteristics to fulfill the operational requirements on information sharing, i.e., which should be the baseline performance of the MIO network?

How do factors such as relative vessel geography, range, mobility, weather conditions and electronic interference affect the network reliability, availability and performance?

D. SCOPE

The scope of this thesis is to coordinate the implementation of the successfully tested technology of the TNT testbed into fully operational MIO capabilities. Since the potential of such technologies and tools have already been explored in the past, the next

step is to develop their incorporation into the MIO missions undertaken by military and law enforcement personnel, in order to satisfy their requirements.

E. METHODOLOGY

- First the boarding party's operational requirements regarding equipment and network performance will be defined covering various possible types of MIO environments.
- Next, the appropriate equipment and network performance metrics will be identified and correlated to these requirements.
- Using the CENETIX testbed, as well as related assets from collaborating organizations, an internet extension to sea will be created during MIO field trials, connecting those organizations to the operational command, the support vessel and the boarding party on board an inspected ship.
- During the aforementioned field trials, boarding procedures will be executed as close to real world operations as possible, providing an insight to the necessary network information flow needs as required, in order to keep the boarding officer to an adequate level of situational awareness and decision making capability.
- Network traffic data will be collected and analyzed using the available network management and monitoring tools such as Solar Winds Engineer's Edition to name one, in order to evaluate that data against the established performance metrics.
- Fault, configuration and performance issues will be identified and corrected for the subsequent field trials.

F. THESIS ORGANIZATION

This thesis is organized in the following way: Chapter I provides an aspect of the problem that lead to this study, as well as the objectives, scope and methodology to be followed. Chapter II briefly describes the different wireless technologies, protocols, network management and monitoring tools and collaboration applications utilized during the field experimentation, in an attempt to address their shortcomings and justify their implementation during the field experimentation. Chapter III validates the operational requirements set by a boarding officer regarding equipment and network performance, as well as collaboration. Chapters IV and V describe TNT 06-2 and 06-3 field trials respectively, along with their conclusions on the network performance, the equipment applicability and the operational requirements gratification. Chapter VI wraps up with the final conclusions, lessons learned and recommendations for future research.

II. BRIEF DESCRIPTION OF UTILIZED TECHNOLOGIES

A. OVERVIEW OF OFDM

Both of the technologies / standards used in TNT experiments for establishing a ship-to-shore or ship-to-ship wireless link (IEEE 802.16 and 802.20, as described later on in this thesis), utilize the OFDM concept. OFDM, a spread spectrum technique often called multi-carrier modulation (MCM) or discrete multi-tone (DMT) modulation (Suitor, 2004), stands for *Orthogonal Frequency Division Multiplexing*, and it is not new: it has been used in IEEE 802.11a/g Wi-Fi standards for quite a while. Actually, OFDM has been known for many years but has only recently become feasible, due to the falling cost and rising complexity of digital circuits and computing power (Olexa, 2005).

OFDM can either be seen as a modulation technique or a multiplexing technique (variation of FDM) and is a special case of parallel transmission. Instead of using one single carrier for transmission, OFDM uses a large number of sub-channels (also called tones). A high rate serial data stream is split up into a set of low rate sub-streams that are then frequency modulated on separate sub-carriers (SC) and transmitted simultaneously to the receiver (Prasad, 2004).

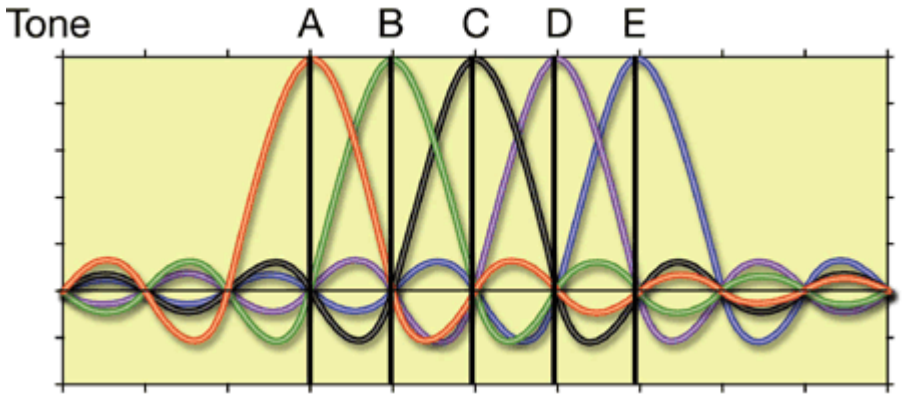

Figure 1. OFDM Tones (From: iec.org)

What discriminates though, OFDM from classical, parallel data / multi carrier systems, is the overlapping of these sub-carriers. Avoiding spectral overlap of the channels to eliminate inter-channel interference is a good idea, however, this leads to

inefficient use of the available spectrum (Prasad, 2004). To deal with the inefficiency of the classical parallel data transmission, OFDM adds the overlapping of the sub-channels.

The following figure highlights that inefficiency of classical FDM systems as compared with OFDM ones: OFDM removes the guard bands between the different sub-carriers and introduces the overlapping among them, thus saving almost 50% of the bandwidth (Prasad, 2004).

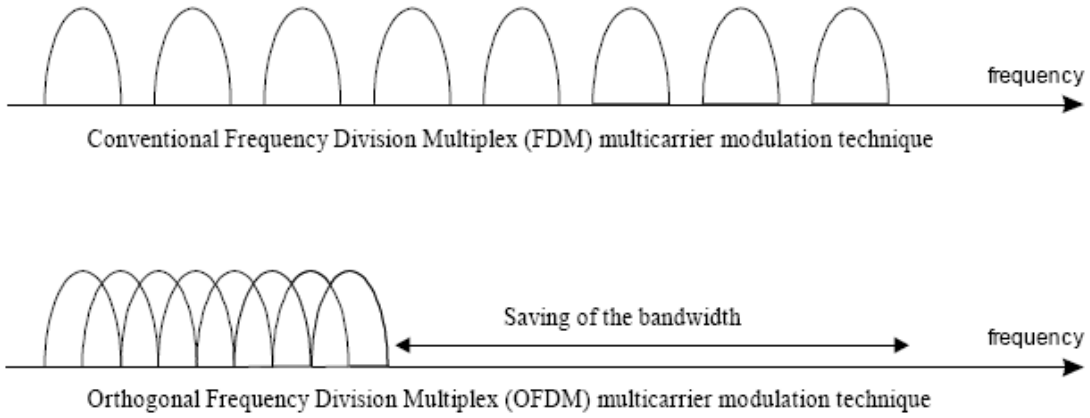

Figure 2. Comparison of the Bandwidth Utilization for FDM and OFDM (From: Technische Universiteit Delft)

Cross talk among the sub-channels can be avoided by introducing a precise mathematical relationship ("orthogonal") between the frequencies of the carriers. The modulated sub-carriers are spaced apart at precise frequencies so that each is centered at the edge of the adjacent carriers. That way, the sidebands of the individual carriers overlap and the signal is still received without adjacent carrier interference. The following figure illustrates the lack of crosstalk from other sub-carriers at the central frequency of each sub-channel.

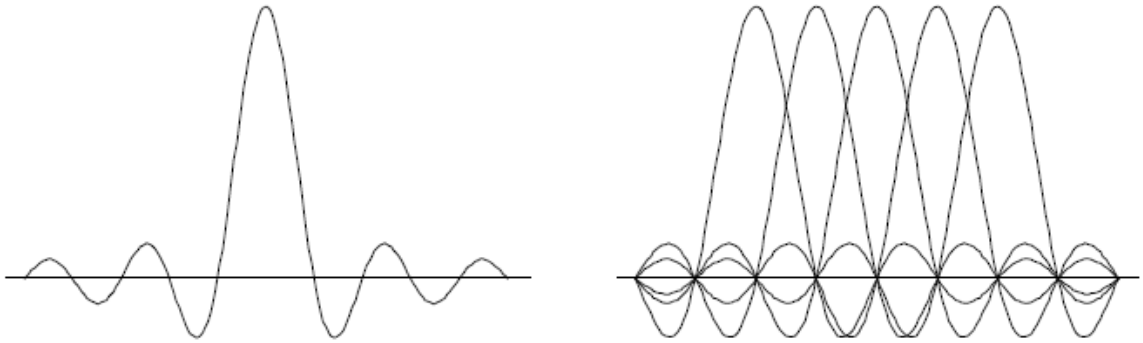

Figure 3. Examples of OFDM Spectrum (a) a Single Sub-Channel, (b) 5 Carriers (From: Technische Universiteit Delft)

The key benefit of OFDM, i.e., higher spectral efficiency, can be better appreciated in licensed spectrum use, where bandwidth can be expensive. OFDM packs more data into the bandwidth compared to a single larger carrier wave or classical FDM parallel data transmission, and thus, delivers "more data per spectrum dollar" (Ohrtman, 2005). Additionally, OFDM has lower susceptibility to another major problem in wireless networks: multipath distortion. Multipath is a phenomenon in which the signal that arrives at the receiver is comprised of the LOS (Line of Sight) signal as well as its reflections on terrain objects that arrive delayed at different times. That causes intersymbol interference (ISI) and degrades the performance of the network. In a single carrier system, interference can cause the entire link to fail, but in a multi-carrier system, only a small percentage of the sub-carriers will be affected as the number of sub-carriers increases. The dispersal of the data stream across multiple channels so that if one channel experiences interference the rest of the data is delivered on other frequencies, reduces the effects of multipath in OFDM systems. Error correction coding can then be used to correct for the few erroneous sub-carriers (Prasad, 2004).

Naturally, OFDM also has trade-offs, the most serious of which is that it has great sensitivity to frequency offset and phase noise (Prasad, 2004). That can be caused by the jitter of the carrier wave and thus requires extremely stable oscillators (Olexa, 2005) or, by the Doppler effect as a result of the mobility of the station. Additionally, its large peak to average power ratio reduces the power efficiency of the radio frequency (RF) amplifier.

1. Overview of IEEE 802.16 (WiMAX)

One of the OFDM technologies being used for establishing a wireless ship-to-shore or ship-to-ship link, as well as for the backhaul TNT network, is the IEEE 802.16 Wireless Communications Standard. Its origins lie in the attempt to substitute the traditional twisted-pair local loop subscriber access with wireless technologies, or as it is more commonly referred to, with wireless local loop (WLL) (http://www.networkworld.com/news/tech/2001/0903tech.html).

The first IEEE 802.16 standard was published on April 8, 2002 as IEEE Standard 802.16-2001 (Air Interface for Fixed Broadband Wireless Access Systems) and is now obsolete; having been superseded along with its amendments IEEE Std 802.16c-2002 (Detailed System Profiles for 10–66 GHz) and IEEE Std 802.16a-2003 (Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz). The current 802.16 standard is IEEE Std 802.16-2004, approved in June of 2004, which is also known as WiMAX (Worldwide Interoperability for Microwave Access), or as WirelessMAN™ (Wireless Metropolitan Area Network) or as Air Interface Standard. Other recently ratified IEEE 802.16 amendments are IEEE Std 802.16e-2005 (Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands – WiMAX mobility standard) and IEEE Std 802.16f (Management Information Base) (http://www.ieee802.org/16/published.html).

802.16 has two main topologies: Point to Point (PtP) for backhaul and Point to Multi Point (PMP) between a base station and subscriber stations, and uses the following frequency ranges: between 10 GHz and 66 GHz (licensed) and between 2 GHZ and 11 GHz (licensed and unlicensed).

There are several reasons for using IEEE 802.16 in TNT experimentation. First, because 802.16 uses the same LLC layer (standardized by IEEE 802.2) as other LANs and WANs, it can be both bridged and routed to them. Second, WiMAX outranges the currently dominant wireless technology by far: it provides a theoretical range of 30 miles compared to the 1000 feet outdoor range of WiFi (http://en.wikipedia.org/wiki/WiMAX). It is also stated that it can provide adequate bandwidth connectivity in NLOS situations, although that should only apply to the lower frequency range, under 6 GHz (Olexa,

2005). Furthermore, WiMAX is capable of very high data rates, primarily because of the implementation of the OFDM concept: while the maximum data rate achieved by WiFi under optimal conditions is 54 Mbps, WiMAX can accomplish 72 Mbps, while its spectrum efficiency can reach 3.6 bps per Hz or higher (Suitor, 2004). Depending on the real world conditions though, the observed data rates are significantly lower.

Another advantage of IEEE 802.16 is located in its MAC layer. IEEE 802.11 already uses contention access (CSMA/CA-DCF), in which all subscriber stations have to constantly compete in order to send each frame through the access point, with its associated "near/far" problem. That problem would be intensified with WiMAX considering that subscriber stations are supposed to be distributed over larger distances. Therefore, WiMAX uses a scheduling MAC (TDMA - Time Division Multiple Access) in which each station is allocated a time slot by the base station. Besides being more bandwidth efficient, that MAC schema allows the base station to control Quality of Service (QoS) by assigning the time slots depending on the needs of the subscriber stations (http://en.wikipedia.org/wiki/WiMAX). If there is only one subscriber station (SS) in the network, the WiMAX Base Station (BS) will communicate with the SS on a Point-to-Point basis. A BS in a PtP configuration may use a narrower beam antenna to cover longer distances (Redline, 2005).

The aforementioned capability of bandwidth on demand (BOD) makes WiMAX ideal for services such as VoIP and streaming video, which, along with its range, equipment portability and bandwidth efficiency makes it also suitable for military applications by extending the battle management network to the frontline nodes. Additionally, and for the same reasons, IEEE 802.16 can be used on behalf of government organizations in humanitarian missions and emergency situations from natural disasters or any other massive destruction of current conventional means of communications.

In order to establish the IEEE 802.16 links, the TNT network uses the Redline Communications AN-50e transceiver / wireless bridge for both fixed wireless backhaul and mobile broadband networks, which has the following specifications:

RF band	5.470 and 5.850 GHz
Channel size	20 MHz
maximum TX power	20 dBm
RX sensitivity	-86 dBm at 6 Mbps
Modulation	BPSK to 64 QAM
Data rate	72 Mbps for both PTP and PMP
Range	> 80 km (50 mi) LOS at 48 dBm EIRP

Table 1. AN-50 Specifications (After: Redline Communications)

Figure 4. Redline's AN-50e (From: Redline Communications)

2. Overview of IEEE 802.20 (Flash-OFDM)

FLASH-OFDM technology has been introduced and developed by Flarion Technologies, Inc., which is now owned by QUALCOMM Incorporated, and stands for Fast, Low-Latency Access with Seamless Handoff Orthogonal Frequency Division Multiplexing, or simply fast-hopped OFDM. The specification for FLASH OFDM is IEEE 802.20, which is a standard for Mobile Broadband Wireless Access (MBWA) and complements IEEE 802.16 in the mobile wireless services area, since the 802.16e mobile standard has not been issued yet. For the time being, IEEE 802.20 and FLASH OFDM are almost synonymous. The key feature of 802.20 is that it is a standard *originally* designed for mobility, in contrast with 802.16e that is designed for fixed broadband access and *modified* for mobility. 802.20 operates in the 400 MHz – 3.5 GHz licensed frequency range, and has a channel bandwidth of 1.25 MHz (Smith and Meyer, 2005). It uses fast hopping across all tones in a pseudorandom predetermined pattern and implements a rate adaptation scheme meaning that, it provides higher data rates when the subscriber is close to the base station (Bahai et al., 2004). According to Flarion, FLASH OFDM is capable of supporting subscriber-base station connectivity and handoff between cells, for platforms moving with up to 250 km/hour.

True mobility support being one reason, and relatively low frequency range of operation the other (resulting in grater ranges and better RF propagation features), make 802.20 very suitable for military applications and especially for the maritime environment. During the TNT 06-2 MIO field trial, the utilized frequency for FLASH OFDM was 700 MHz and the EIRP was 20 W, allowing for satisfactory connectivity at distances of three nautical miles, at almost NLOS conditions.

B. OVERVIEW OF ULTRA WIDE BAND

One of the implemented technologies in TNT experimentation for establishing a wireless network among the boarding party members onboard the inspected vessel is Ultra Wide Band (UWB). UWB, a physical layer technology, is known from the early radio communication years; in fact it was first implemented by Marconi with his Spark gap radio for transmitting Morse code. In recent years, UWB has been used for military radar and covert communications (Nekoogar, 2006), while its special characteristics, indicate that it is very suitable for communications in a Maritime Interdiction Operations (MIO) environment.

Unlike traditional narrowband/wideband communications systems, in which the information signal modulates a continuous waveform of a specific carrier frequency, UWB uses carrierless, extremely short duration pulses at the range of nanoseconds (10^{-9} seconds) or picoseconds (10^{-12} seconds), with a very low Duty Cycle (< 0.5%). According to the Fourier transform, the shortest the duration of the pulses, the wider the bandwidth they spread their energy, which is illustrated in the following figure:

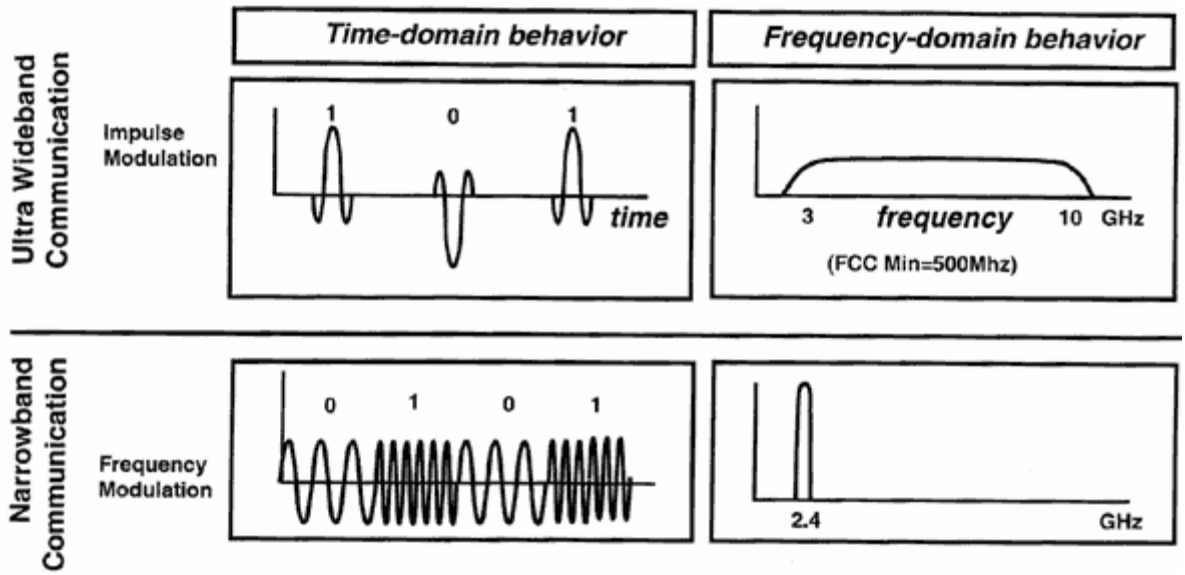

Figure 5. Comparison of UWB and Traditional Narrowband Time and Frequency Domain Energy Distribution Graphs (From digit-life.com)

As a result, while in narrowband or wideband signals, the bandwidth is in the range of MHz, in UWB it is in the range of GHz. Specifically, in order for a communications system to be classified as UWB by the Federal Communications Commission (FCC), it must occupy a fractional bandwidth of 25% or greater or a bandwidth of 500 MHz or more (Intel, 2006). For example, an UWB signal centered at 2 GHz would have a minimum bandwidth of 500 MHz and the minimum bandwidth of a UWB signal centered at 4 GHz would be 1 GHz (Palowireless, 2006).

Also, according to the Hartley-Shannon formula: $C=W\log_2(1+SNR)$, where C=channel capacity, W=bandwidth, and SNR=Signal to Noise Ratio, achieving high data rates is possible because the spectrum is very wide, while the channel capacity increases linearly with the used bandwidth (Bahai et al., 2004). Indeed, UWB promises to deliver very high data rates, currently at the range of 40 to 60 Mbps (although at short distances) and eventually up to 1 Gbps (Webopedia, 2006).

Based on the aforementioned exclusive characteristics, UWB technology is also known as “carrier free”, “baseband”, “impulse” or “nonsinusoidal” technology. The resulting advantages and drawbacks of UWB over narrowband or traditional wideband signals are the following (Nekoogar, 2006):

- Low average transmission power, which leads to longer handheld equipment battery life.
- Very low power spectral density (PSD) (transmitted watts of power per Hz of bandwidth) which translates into low probability of interference to other signals operating in the same band.
- Capability of sharing the frequency spectrum with narrowband and wideband radio services and unintentional radiators because UWB communications reside below the noise floor of these transceivers.
- Large channel capacity (data rate) as previously described, resulting in the ability of transmitting high definition streaming video.
- As explained by the Hartley-Shannon formula, UWB provides the ability to work with low SNR's; because bandwidth is high, SNR can be small but still providing us with high channel capacity, which eventually translates into high performance in noisy environments.
- Low probability of Intercept and Detection (LPI/D). Practically, UWB provides immunity to detection and intercept because of the very low average transmission power (eavesdropper must be very close to the transmitter) and also because UWB pulses are time modulated with codes unique to each pair of transceivers and therefore it is very difficult to determine when the extremely narrow pulses will arrive. However, UWB's difficulty to detect also results in a difficulty for FCC to regulate its transmissions.
- Resistance to jamming because of the frequency diversity as a result of the high processing gain (PG = RF Bandwidth / Information Bandwidth). It is not possible for a jammer to jam every frequency in the UWB spectrum and thus a great percentage of UWB's spectrum will not be affected which translates into survivability in hostile environments.
- Immunity to multipath. The very short duration of UWB pulses diminishes the probability of reflected non-LOS pulses to collide with the LOS ones; the direct path signal has come and gone before the reflected path signal arrives at the receiver.
- Obstacle penetrating capabilities because of the low frequencies included in the broad range of the UWB frequency spectrum (long wavelengths).
- Simple transceiver architecture: UWB transmission is carrierless, which translates into fewer RF components transceivers (no need for power amplifier, mixer and local oscillator). That results in lower complexity, lower cost and higher MTBF (Mean Time Between Failures) transceivers.
- Very complicated channel estimation because of the difficulty to predict the template signals.

- High sensitivity to timing errors such as jitter and drift; the transceiver must be able to detect the exact position of the received signal and thus, there is need for precise synchronization and high speed ADC's.
- Multiple user access in an UWB network is very challenging because the detection of the desired user's information is much more difficult than in narrowband communication.
- Finally, the major drawback of UWB, due to the low transmission power, is the short range.

The present UWB applications are, according to its aforementioned special characteristics: accurate positioning and fine radar range resolution, through wall imaging (for MOUT warfare), ground penetration radar (for rescue operations), and high data rate, short range WPAN's (Wireless Personal Area Networks) for replacing the wires that connect computers and peripherals. Specifically, UWB is ideal for communications inside a ship's hull because of its metal penetration capabilities, its high data rates that provide the ability to transmit excellent quality streaming video, and its immunity to multipath.

C. OVERVIEW OF MESH NETWORKS

Another network topology that is utilized on board the inspected vessel, in order to provide wireless connectivity to the boarding party members that are dispersed on the deck of a ship, is mesh topology. A self forming, self healing, mesh network in which nodes associate in an ad hoc manner, provides enormous advantages over the infrastructure mode of traditional wireless networks:

1. Self Healing Behavior

Mesh networks have a self-healing behavior: instead of having all nodes associated only to the access point (as in infrastructure mode), in mesh topology (as in ad hoc mode), each node is connected to all the others. As a result, there is no single point of failure; data from one node has many alternative paths to "hop" to the final destination. Even when one node is down, or when a link is congested, the network remains operational, thus increasing its redundancy and reliability. That reliability increases even more, as more nodes are added to the network, because more nodes translates into more possible routes for data to travel.

2. Greater Range

The operation of nodes as repeaters, allows stretching the network to greater distances and bypassing obstacles that block the signal. This is extremely convenient for the maritime environment especially on board a ship, where metal constructions would otherwise obscure connectivity.

3. Higher Throughput

Unlike infrastructure mode wireless networks, where all stations connected to the same access point have to share a fixed bandwidth, with mesh topology, the more nodes on the network, the more available bandwidth there is in total, provided of course that the topology of the network and the routing algorithm are such, as to minimize the number of hops, and provide the most suitable path from node to node. Furthermore, since the distances between the mesh nodes are usually shorter than the ones between subscriber stations and base station, the associated links can operate on higher data rates, thus increasing even more the total throughput.

During TNT MIO field trials, the IEEE 802.11 standard in mesh configuration was initially used, to be replaced later by ITT, a proprietary wireless mesh technology of Motorola.

THIS PAGE INTENTIONALLY LEFT BLANK

III. OPERATIONAL REQUIREMENTS FROM NETWORKS USED IN MARITIME INTERDICTION OPERATIONS

War against asymmetric threats is a global war that is not constrained inside borders or battlefields and therefore, it has to include multiple law enforcement or homeland security agencies as well as military forces and commands from various countries. In order to succeed, all the participating forces must coordinate and share information in a timely and reliable manner. Under the present circumstances though, it is very difficult to establish a common operating environment among all the participants. That difficulty can be located mainly in the difference between policies, procedures, budget, capabilities, and technologies used for acquiring and transmitting or sharing the necessary information. That fact, not only applies between different countries, but even to different organizations inside the same country. As a result, the war fighter, whether at operational or tactical level, often does not have the right information at the right time in order to make the right decisions. Hence, the key objective of a network used for Maritime Interdiction Operations, would be the ability to provide to the Coast Guard or SOCOM operators, all the necessary means to exchange any required information with their respective higher authorities and collaborative organizations, reliably, timely, securely, and effectively. In order to achieve this, a series of operational requirements need to be fulfilled, pertaining to all aspects of a boarding operation and dealing with the following factors:

- Sufficiency, portability and easy setup of the network equipment
- Network scalability and user training requirements
- Coping with constraints posed by the operating environment, such as weather, range, visibility, and electromagnetic interference
- Level of situational awareness that is required in order to make certain decisions

In detail, the operational requirements of such a network are analyzed below.

A. POWER AND WIRED CONNECTIVITY REQUIREMENTS

The basic assumption for deploying a MIO network is that there is no infrastructure on board the inspected vessel that can be used by the boarding party members. That worst case scenario requires that all hardware must be self sustained in

matters of power and connectivity. Wired connectivity issues are easily resolved with CAT-5 cables of various lengths, carried along with the rest of the equipment of the search party. Additionally, laptops, wireless bridges, antennas and switches must be able to run on batteries for a time period that is difficult to determine since it depends on the size of the target vessel to be searched, as well as on the findings of that search. Rule of thumb, based on boarding experience, dictates that the battery life of all hardware should be enough to power up the devices for a minimum of 8-10 hours (which is an approximate time required to search a large Ro-Ro vessel). That problem has been successfully faced during TNT 05-4 experiment, where the required power for the ship-to-ship link equipment (Redline AN-50 wireless bridge) was provided by Mil-5590/390 12/24 volt batteries (Marvin, 2005). In the case of a boarding that lasts longer than usual, additional batteries can be carried by the boarding party. This can be done for the laptop batteries, as well, that definitely have a shorter duration battery. Furthermore, the self power sustaining requirement of the boarding party equipment diminishes the constraint of placing the devices close to power outlets, something that could possibly limit the LOS of the antennas.

B. NETWORK DEPLOYMENT TIME REQUIREMENTS

Another assumption for deploying a MIO network is that the target vessel has already been secured, perhaps by an assault team in the case of a non-complaint boarding. In any case, the network cannot be setup by the same boarding party members that have the task of securing the ship. An additional number of 4-5 personnel are required in order to do that, and the time needed is approximately 15 minutes, including the set up of both the ship-to-ship link and the on board LAN's, as measured in TNT 06-1/2 MIO experiments. That time is less than the minimum that could be possibly required by a boarding officer, since just the preliminary search process of the vessel, i.e., gathering and checking of the vessel's and crew's documents and passports, requires more time. In order to keep the network deployment time low, though, information must be provided to the boarding party prior to the execution of the boarding, such as blueprints and photographs of the ship, so that the decision of where to set the antennas and consequently the rest of the equipment, is pretty much made prior to the actual boarding. That would also help in the actual boarding process / search phase of a vessel. The arising

requirement in that case, is to have the boarding party or their launch vessel already on a data network with MIFC or other relevant organization that can provide such information immediately upon request.

C. EQUIPMENT PORTABILITY REQUIREMENTS

This requirement has been dealt with in past TNT experiments with success. The total weight of the required equipment does not exceed 60 pounds, while its volume allows loading and carrying it in two US Alice, large backpacks or similar rucksacks, by the additional boarding party members required for setting up the network. Perhaps, two pelican cases would be even better since they can provide shockproofing and waterproofing for the networking equipment during its transportation. The typical list of equipment includes:

- A number of laptops with the following tasks:
  - UWB LAN access point
  - Radiation detection data uploading/gathering
  - ITT mesh network access point
  - GPS receiver/poster
  - Biometrics data gathering
  - For the collaboration between the boarding officer and the rest of the nodes (Groove)
  - For network management and monitoring (Solar Winds)

Even by having laptops with dual purpose (i.e., the same for ITT mesh network access point and GPS receiver/poster), the total number of laptops that are required cannot be less than five.

- 1 Redline AN-50 wireless bridge with antenna, RF cable and power supply
- 1 eight-port (at minimum) switch with several various lengths CAT-5 cables
- UWB antenna and connector
- ITT mesh AP with power supply
- One or more network video cameras

D. RANGE REQUIREMENTS

In terms of range, the wireless links used for ship-to-ship or ship-to-shore connectivity, must be able to provide high throughput data rates in over-the-horizon distances. The reason is that when dealing, for example, with radiological material, the threat interdiction has to be performed at the safest possible distance from the homeland. Additionally, there are cases where the launch platform must stay beyond radar and visual detection range from the target vessel, in order to maintain the element of surprise, in the case of a non-compliant boarding on a High Value Target (HVT). After the seizure and control of the target vessel, the launch platform will be able to close in, but at least at the initial stages of the wireless link setup, the distance will still be beyond the visual and radar horizon. An indicative visual / radar range in that case, estimated for an average bridge / antenna heights of 30 feet, for both launch and target vessel, would be:

Radar LOS = $1.23\sqrt{30}$ ft + $1.23\sqrt{30}$ ft = 13.47 nautical miles (nm)

Optical LOS = $1.06\sqrt{30}$ ft + $1.06\sqrt{30}$ ft = 11.61 nautical miles (nm)

The above distances are close to 12 nm, which is the internationally established territorial waters range, in which a country has the jurisdiction of performing boardings without the need of United Nations sanctions. Furthermore, in cases where the target vessel is suspected of carrying radioactive material, there might be a safety requirement of conducting the boarding as far away as possible from the shore. Based on the aforementioned reasons, the network range requirement mandates that the link should be able to perform reliably at an approximate range of 12 nm.

E. "ALL CONDITIONS" EQUIPMENT REQUIREMENTS

This requirement is two-fold: it has to do with two possible constraints such as weather conditions and night operations.

First, when weather conditions allow for the safe conduct of a boarding, the networking equipment should not be a limiting factor. Weather considerations on the MIO network capability to perform reliably are posed by sea state, and humidity / rain. These factors might not necessarily suspend boarding operations, but might pose a serious bottleneck on both the ship-to-ship / ship-to-shore link as well as on the onboard LAN's.

Apart from the antennas certified for outdoor use, so far, none of the TNT MIO network equipment is waterproof or even weatherproof. That issue not only creates problems on the transportation of the equipment onto the target vessel, but also restricts the setting of the network equipment only in closed spaces when the weather is humid or rainy, which in turn affects the placement of the antennas and thus creating connectivity issues. Therefore, the weatherproofing of the network equipment is a necessary requirement since it provides true portability.

Another weather variable that affects the reliability of the MIO network is the sea state conditions. Depending on the antenna lobes used for ship-to-ship / ship-to-shore link, a high degree of pitch and roll, although not prohibiting the conduct of the boarding, might degrade the performance of the link, even up to the point that no communication might be possible at all. There is a tradeoff between the gain and the susceptibility of the antenna to that factor. Narrow beams provide longer range, better signal strength and higher throughput connectivity but, on the other hand, that is only possible in calm water conditions. In case of using self aligning antennas, the aligning mechanism must be able to respond quickly in order to follow the pitch and roll of the vessel. Since the specifications of such antennas are still unknown, the best solution for now would be to have two or three antennas for the boarding party (directional with different sizes/lobes, omni), in order to choose the best one for the occasion.

The second requirement has to do with night operations or with limited visibility, whether day or night. Even with normal visibility conditions, when the distance between the target ship and the support vessel or the land is increased beyond visual range, the major issue is the antenna orientation. So far, the alignment of the antennas during the field trials has been successfully performed visually and with the aid of Redline's RF Link Monitoring Tool. However, the conditions during these field trials were ideal: conducted in daytime, with a range of less than two nautical miles, and with a distinct visual LOS between the two antennas. Real world scenarios, though, include nighttime operations in heavy ship traffic, or adverse weather and low visibility, in which not just the antenna is not visible but the whole target vessel, as well. In such cases, the antenna's alignment would not be possible with the tactics that have been followed so far. The need

for self aligning antennas becomes imperative, or otherwise there is need for a support vessel to be very close to the target vessel, something that is not always possible.

F. NETWORK SCALABILITY REQUIREMENTS

In a world that is advancing at a much faster pace than in the past, it is very difficult to set fixed requirements, especially for military projects that also involve other government organizations. Apart from the technology that is changing, threats and objectives change continuously, as well. Consequently, one of the requirements for the MIO network is scalability, in order to be able to follow the technological advances in wireless networking and collaborative tools, as well as being able to include more nodes as necessitated by future requirements, i.e., expand its collaboration environment. That is made possible by the use of commercially available technology for the hardware and software of both the networking and the collaboration equipment. On the other hand, that it is a major bottleneck when strictly military technology is being used: upgrading of the equipment at certain periods after the initial deployment, requires unreasonable time and budget, since it solemnly depends on military equipment vendors. Furthermore, strictly military technology would require specialized training of the users, while many nodes that reside outside the US military community, either domestic civilian or international, would be excluded since they would not have the necessary security clearance to own and use the specific military technology. The use of commercial technology does not pose these obstacles because it allows for the quick integration of organizations into the MIO network since equipment and know-how are already available to everyone.

Today, the use of commercially available technology in TNT MIO networking equipment satisfies the aforementioned requirement. More nodes are being added to the network providing the boarding party with real time information and expertise, without the need for additional training, and with already existing or low acquisition and upgrading cost technology.

G. ELECTROMAGNETIC INTERFERENCE (EMI) REQUIREMENTS

So far, during the TNT MIO experimentation, EMI has not been a concern. Vessels that were used either to launch the boarding party or as a target ship, were equipped with I-Band navigation radars operating approximately at the 9 GHz range, and thus did not interfere with the 802.16, 802.20 or other TNT MIO transmitters.

Furthermore, these vessels did not have voice or data communication networks other than their usual marine VHF radios. As a result, EMI has not been tested yet, although it can be a major problem onboard or in the proximity of warships. It is not uncommon for a boarding team to be launched from a warship, and relay boarding information through that warship which remains close to the target vessel for general support issues. Warships operate several radars simultaneously, in a great variety of frequencies, with an output power of several KW and for several purposes (navigation, surface / air surveillance, tracking targets), not to mention their infrastructure of communication networks, also in a wide frequency spectrum. For example, radars found on warships such as the SPS-10 surface radar and the MW-08 target indication radar, operate in the vicinity of 5.8 GHz of Redline's equipment. Therefore, EMI in a real operational scenario should be very thoroughly considered; even if it is not possible to eliminate all interference sources, at least we need to know the specific emitters that interfere with the ship to ship link as well as the mesh network. As a safeguard, special procedures can be issued to avoid the interference such as sector transmission for radars, lower output power or use of other means of surveillance and communications. As described in the previous chapter, UWB is practically invulnerable to interference, due to its unique characteristics (very low power spectral density - PSD).

H. COLLABORATION, SITUATIONAL AWARENESS, AND DECISION MAKING REQUIREMENTS

Sufficient collaboration, maximum situational awareness (SA), and correct decision making capability are the ultimate goals not just of the TNT MIO network, but in general, of Network Centric Warfare (NCW). The most significant among these three goals, is SA because it is the link between the other two; SA is the basis for correct decision making, especially in complex and dynamically changing environments, and it is a byproduct of sufficient collaboration among the decision makers and those who own the required information, either operators or experts.

The first use of the term "situational awareness" originated in the naval aviation community to describe a pilot's understanding of what is going on around him during aircraft dog fights. Naval Aviation Schools Command refers to SA as: "the degree of accuracy by which one's perception of his current environment mirrors reality,"

(https://wwwnt.cnet.navy.mil/crm/crm/stand_mat/seven_skills/SA.asp). Further analysis, identifies SA as being a function of identification and processing of available information, resolution of the relative importance of critical pieces of information, correlation of the critical information with the objectives of the decision maker, and anticipation of what is most likely to happen next. After defining SA, it becomes obvious that in order to investigate the relevant requirements of the TNT MIO network, we need to determine the necessary collaborative environment that is sufficient to provide SA; in other words we need to determine the "logical" structure of such a network, answering questions not only about nodes but especially about links among these nodes and traffic content as well:

- Which should be the nodes of the network, i.e., who will benefit from such a network, and who needs to be included in the collaborative environment?
- Which should be the links and what kind of decision making structure is the most appropriate for the MIO environment, in order to fully exploit the provided capabilities of the technology?
- What kind of data is going to be shared through that network, i.e., which is the context, type, volume, frequency, originators and recipients of the network traffic?

1. Network Nodes

Apart from the obvious nodes of the boarding party (boarding, biometrics, and radiation officer), the selection of the rest of the nodes of the MIO network, depends on their possession of the necessary expertise or knowledge, as well as on their contribution to the decision making process; in other words it is all the personnel that a boarding officer would like to virtually have in the boarding party. Moreover, it is the whole infrastructure that is behind these personnel: laboratories, databases, decision support systems, combined knowledge, networks and IT systems. So far, the existing nodes include only a small subset of the required information holders, since the field trials have been conducted in the restricted environment / scenario of the San Francisco bay area, as described in subsequent chapters. Looking at a generic MIO environment, trying to cover all possible aspects, we can produce the following list of required nodes:

a. Coast Guard Intelligence Departments

Maritime traffic information includes ships' registries, cargo and crew manifests, ports of call, and shipping schedules. That kind of information is helpful in order to designate a vessel as suspect, locate it, make its interdiction possible, and confirm discrepancies onboard, such as fake documentation. Bearers of such information are port authorities and shipping companies who usually report to pertinent Coast Guard departments. That definitely justifies the presence of MIFC (Maritime Intelligence Fusion Center) as a network node, as well as any other similar, domestic or international, agencies involved in law enforcement in the maritime domain.

b. Experts in WMD

Weapons of Mass Destruction (WMD) expertise involves the ability to detect them, reveal their identity, categorize them, trace their origins, correlate their profile with other related findings, and evaluate the associated dangers and implications from their discovery. That expertise includes also the identification of certain materials that can lead to the development of WMD, such as machinery and other non-proliferation materials. There is no way for a boarding party to be able to do all these, even if the best scientists were on board the suspect vessel. A better term to use instead of experts is, centers of expertise; that way it includes not just the people but also the infrastructure that supports them.

For the time being the boarding party alone, can detect the presence of radiation under certain circumstances. That indication though, is not enough to designate a vessel as suspect; specific materials that emit radiation are lawfully used on board ships, such as old smoke detectors, tank level indicators and gauges. The key point is that the boarding party members do not have the ability to evaluate or even comprehend their findings on board the target vessel; they cannot provide answers on what the identity of the radiation source is, what it is used for, or what the associated dangers for themselves and the surrounding area are. Hence, they are not in a position to make decisions by themselves. It is therefore obvious that centers of WMD expertise should be the primary nodes of MIO networks, whether being experts on nuclear (so far), or biological and chemical materials (in the future), and their assigned role is to provide answers to the aforementioned questions.

c. Experts in IED's

As mentioned earlier, one of the assumptions for setting up and operating a MIO network, is that the suspect vessel is already secured. That security, though, only refers to crew and ship's compartments. It means that the crew members have been detained, if necessary, and that all compartments have been checked to verify that there are no passengers hiding in them; there is no provision for possible dangers associated with booby-trapped hidden material and the clearance of Improvised Explosive Devices (IED's). The boarding party, once they have detected that material, would request remote expertise assistance before tampering with it. That would be the wise thing to do for their personal protection as well as for the protection of a certain area around them. Again, even if EOD specialists were included in the boarding party roster, their abilities would be limited without their supporting infrastructure. That would only be possible by having them as nodes in the MIO network.

d. Emergency Medical Assistance Advisors / Coordinators

That node provides expertise on the associated dangers related to the discovery of WMD or their construction materials. In other words it faces considerations such as the danger to the boarding party members from having been being close to certain WMD sources, or the possible required medical treatment to them after that has happened. It can also provide a first assessment of the necessary precautions for the entire surrounding area of the boarding, in collaboration with the WMD experts, and coordinate the actions of various relevant state organizations, in order to comply with these precautions. Anyhow, even without a positive WMD detection, just the suspicion of WMD presence, definitely warrants the emergency medical assistance advisors / coordinators as nodes in the MIO network.

e. NBFC / Biometrics Databases

Biometrics information is necessary to the boarding party in order to discover whether crew members of the boarded vessel are included in the lists of terrorist or common criminal databases. A remote access to these databases is enough, without the need of human collaboration, provided that the boarding officer can be interfaced directly with these databases, and that the response from them will be either a hit or no hit. All other responses from the databases would require human collaboration between the

boarding officer and personnel with biometrics expertise. For example, an answer such as "75% hit possibility" might not be sufficient to justify certain subsequent decisions for the boarding operation. One way or another though, having nodes in the MIO network such as the NBFC (National Biometrics Fusion Center) is absolutely justified. For the time being only fingerprints biometrics data is utilized; it is just a matter of time to include other biometrics identification capabilities, such as facial recognition, which might require the addition of more nodes to the MIO network.

f. Law Enforcement Authorities

The vast majority of boarding operations are not executed with the objective of discovering WMD, but mainly for law enforcement purposes: counter narcotics, smuggling, and trafficking operations as well as weapons embargo enforcement are the most common objectives. In such cases, instead of WMD expertise, the boarding party needs to collaborate with relevant authorities that monitor such illegal activities, and have databases and expertise to support the discovery of suspect vessels and their illegal cargo. In that category of nodes falls MIFC as described earlier in this chapter, as an owner of maritime traffic intelligence. Depending on the kind of the boarding party's mission and origins, there can be a lot more nodes to be included in the MIO network that apply to each different case: DEA (Drug Enforcement Administration) for counter-narcotics operations, JAC (Joint Analysis Center) Molesworth for embargo operations by NATO warships, and so on.

g. Networking / Technical Advisors

It is not possible for the boarding party members to have the expertise to deal with complex networking problems that might arise at any point of the boarding operation and obstruct them from exploiting the unique capabilities offered by the network. Their abilities on that subject only include training to face common issues that may have been revealed during the experimentation phase. There would be no difference if they were using voice radios; they would know how to set them up, operate them, and probably how to troubleshoot them, but they would not be able to repair them or monitor their performance. Thus, a MIO network node should have that role, other than the boarding party, that would be able to collaborate and advice the boarding officer on

networking issues, and at the same time to monitor the network performance utilizing the appropriate protocols and network monitoring tools, and act preventively.

h. Tactical / Operational Commanders

There would be no benefit in the MIO network if the primary decision makers were not included in it. Most of the decisions before and during the boarding phase, and definitely on what should happen after the findings on the suspect vessel have been evaluated, are made by the tactical or operational commanders at their respective levels of authority. The boarding officer is their "tool" onboard the ship, making decisions on the lowest level, following the SOP's: how to organize and conduct the search using the best resources at his/her disposal. The decision making level of the tactical or operational commanders may differ depending on the context of each boarding case, their parental organizations, relevant policies and standing orders. The common factor though is that they need to be a part of the network and have the ability to collaborate directly with just one degree of separation (at least for the tactical commander) with the rest of nodes. Perhaps, enhancing their situational awareness might be more important than that of the boarding officer.

2. Network Links

Once the necessary nodes of the MIO network have been defined, the next consideration is how to link them in order to produce the optimum collaborative environment for the decision making process at hand. In other words, which would be the most appropriate network and decision making structures for the MIO environment, in order to fully exploit the provided capabilities of the technology and achieve maximum situational awareness? The answer to that question is based upon the special characteristics that govern the MIO network:

- The decision making nodes do not posses the information to make the decision, while other non-deciding nodes posses critical expertise to base the decision on
- The context of the problem is highly unstructured, non-routine and might change on a case by case basis
- The setting of a specific collaborating environment that matches a case, might be ad hoc, since not all the parameters of the problem are known from the beginning

- There might be a need for innovative solutions, not considered before the boarding operation
- In certain cases, the importance of the decision is critical

The aforementioned reasons lead us to adopt the committee-type decision making structure (Figure 6), while the network communication structure in that case should be completely connected.

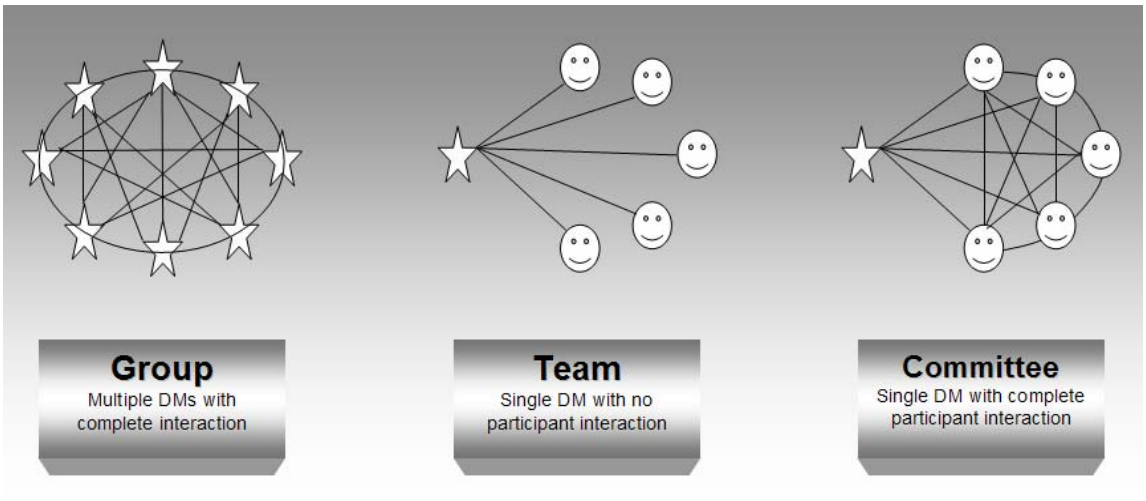

Figure 6. Basic Multi-Participant Decision Making Structures (From: Marakas, 2003)

Indeed, the way the MIO decision process works, is via collaboration among all the nodes; a complete interaction is required because a node might hold the critical piece of information that can lead to the correct decision at a given moment. That piece might not be revealed, unless triggered by an interaction with another node, which will not be possible unless each node is connected to all the others. So far, Microsoft's Groove Virtual Office has proven very suitable for that case, until something better comes along.

3. Collaborative Traffic Context

Hayes-Roth (2006, 105) provides a list of the smartest things that must be done in order to reduce communication traffic, while achieving better coordination. That list applies directly to the context of the messaging and the nature of collaboration. It is common sense that one of the requirements of the MIO network should be the reduction of the traffic, not just for minimizing bandwidth requirements, but also because traffic

overload of a network has a negative impact on the cognitive process. Based on this list, we can extract the requirements of the MIO-specific case that pertain to the context of the exchanged information.

a. Adoption of a Standardized, Unambiguous Set of Messages

As justified in subsequent chapters by real examples from the field trials, the standardization of the collaboration messaging plays a critical role in the cognitive process. Unless all the participants decide and follow standard messaging, there is an equal chance that not situational awareness, but confusion might be induced instead. First, a standard naming convention of the posted files, either biometrics, radiation spectrum files, or other, must be adopted, in order for the participants to be able to know:

- what kind of information they contain
- what does that information pertain to
- when was that information obtained, i.e., what time and in what order (illustrating the history of events)

Second, standardization in the text messages must be followed, reducing the risk of misunderstandings due to the different meanings people give to the same words or phrases. That issue becomes even more prominent, considering the educational differences of the participating nodes as well as their spreading worldwide.

b. Communication of Information that Is Needed and Can Be Understood Only

Again, as proven later on in the subsequent chapter of the TNT 06-3 field trial, there is no good in sharing information that is not needed or cannot be processed by the other nodes, at least in the time frame available. It can only cause delays in the cognitive process, creating additional responds and replies among the nodes, and that leads us to the next requirement of the MIO collaborative environment:

c. Separation of the Collaborative Environment into Domains or Clustering of the Nodes

In order to reduce the "globally" visible traffic of the MIO network, a separation of the nodes into clusters or workspaces is necessary. Nodes that interact mainly with a number of other nodes should be clustered separately into different workspaces. That would increase the degrees of separation between certain nodes from one into two, but a low degree of separation is not always desirable, as the number of

nodes and subsequently the network traffic, increases. As an example, the different departments of an expertise organization, such as LLNL, could be collaborating in a different workspace, having only one representing node in the other workspaces.

4. Video Feed from the Target Vessel

So far, in many boarding operations throughout the world, and especially in offensive board and seizure of a ship in the case of non-compliant boardings, one or more cameras are used by the boarding team, in order to capture all the events that take place during the operation on board the target vessel. That mainly has to with the legal protection of the boarding team, in order to have proof that their specific actions were justified by what was happening, such as excessive force. Additionally, the same video recording is used for data collection, although it cannot be processed in real time to extract useful information. In MIO field trials, the same concept has been extended to the transmission of the video stream in real time to video conferencing workspaces that all the necessary participants can view, and advice the boarding officer based on what they see in real time. The boarding party operational requirement in that case will be fully satisfied if the video feed is obtained from mobile nodes instead of fixed, i.e., if the cameras are recording what the boarding party members see throughout the ship, instead of providing stationary views of certain ship's spaces.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TNT 06-2 FIELD TRIAL

A. EXPERIMENT SCENARIO

The scenario of the TNT 06-02 experiment for Maritime Interdiction Operations was a very possible, real case scenario that concerns all agencies and institutions involved in homeland security operations and especially those related to maritime interdiction, interception and control. Briefly, the designed course of events was as follows:

- According to intelligence, a cargo vessel, whose name is unknown, is carrying a terrorist cell with hazardous (radiological) material and is about to approach a Pacific U.S. coast port (also unknown).
- Under that information, multiple boarding operations are ongoing on maritime traffic approaching Pacific U.S. coast ports.
- A USCG cutter (simulated by MARAD SS Gem State) is ordered by USCG Operations Center to stop, board, and search a merchant vessel (simulated by USCG Tern) at the proximity of a U.S. west coast port.
- In order to do that while the suspect vessel is underway, a RHIB with a boarding team is employed.
- During the initial inspection, the Level I boarding team's RadPagers detect some source of radiation.
- A Level II boarding team is employed in order to resurvey the ship with their additional radiation detection equipment, as well as to identify the crewmembers using biometrics recording devices.
- In order for the boarding team to evaluate their findings while the target vessel is still underway, a reach back capability is required, to centers of expertise such as the Lawrence Livermore National Laboratory (LLNL) for radiological data and the National Biometric Fusion Center (NBFC) for biometrics data.
- The aforementioned capability is provided by a rapidly deployable network extension, from shore-to-ship (from MIFC/USCG Island to SS Gem State) and from ship-to-ship (from SS Gem State to USCG Tern).
- Additionally, onboard the inspected vessel, the network must be further stretched, in order to provide wireless connectivity between the boarding party members, whether on deck or inside the ship's hull.
- Under that course of action, the boarding party sends radiation spectrum data files as well as fingerprint data files for analysis. At the same time, a continuous video stream is being transmitted from the inspected vessel,

providing the support ship, the operational command and all the collaborating agencies with a real time view of what is going on the inspected vessel.

- Once the findings are analyzed and radiation and biometrics data is identified, the respective agencies send a response back to the boarding officer, which is also "visible" to the operational command (MIFC), allowing them to decide on the correct course of action.

B. EXPERIMENT OBJECTIVES

The experiment's objectives were many-fold:

- Explore the potential and arising problems of establishing ship-to-ship, ship-to-shore and inside the ship wireless data connectivity, using the available wireless technologies (IEEE 802.16 - 802.20 - ITT - UWB).
- Investigate the reliability / performance of those links to transfer the required data uplink / down link (in terms of throughput, latency, and jitter) by using the available network management tools.
- Assess the feasibility of the utilized applications (Groove virtual office) of providing the boarding team, the operational command and collaborating agencies with a common operational picture and situational awareness.
- Assess the frequency of messaging, the amount and type of data required to be transferred in order to provide situational awareness.
- Measure the time needed by the remote collaborative agencies of expertise, to receive and acknowledge viewing of shared data, analyze it and come up with an answer.

C. NETWORK TOPOLOGY

During the boarding operation, all four aforementioned wireless links / technologies (802.16, 802.20, UWB, ITT) were used in order to exchange data between the boarding party (aboard the inspected vessel or the RHIB) and the launch vessel, or among the members of the boarding party. The following two figures illustrate the network between the GEM STATE and USCG TERN (network extension at sea) as well as the backhaul network to the distributed centers of expertise and operational command:

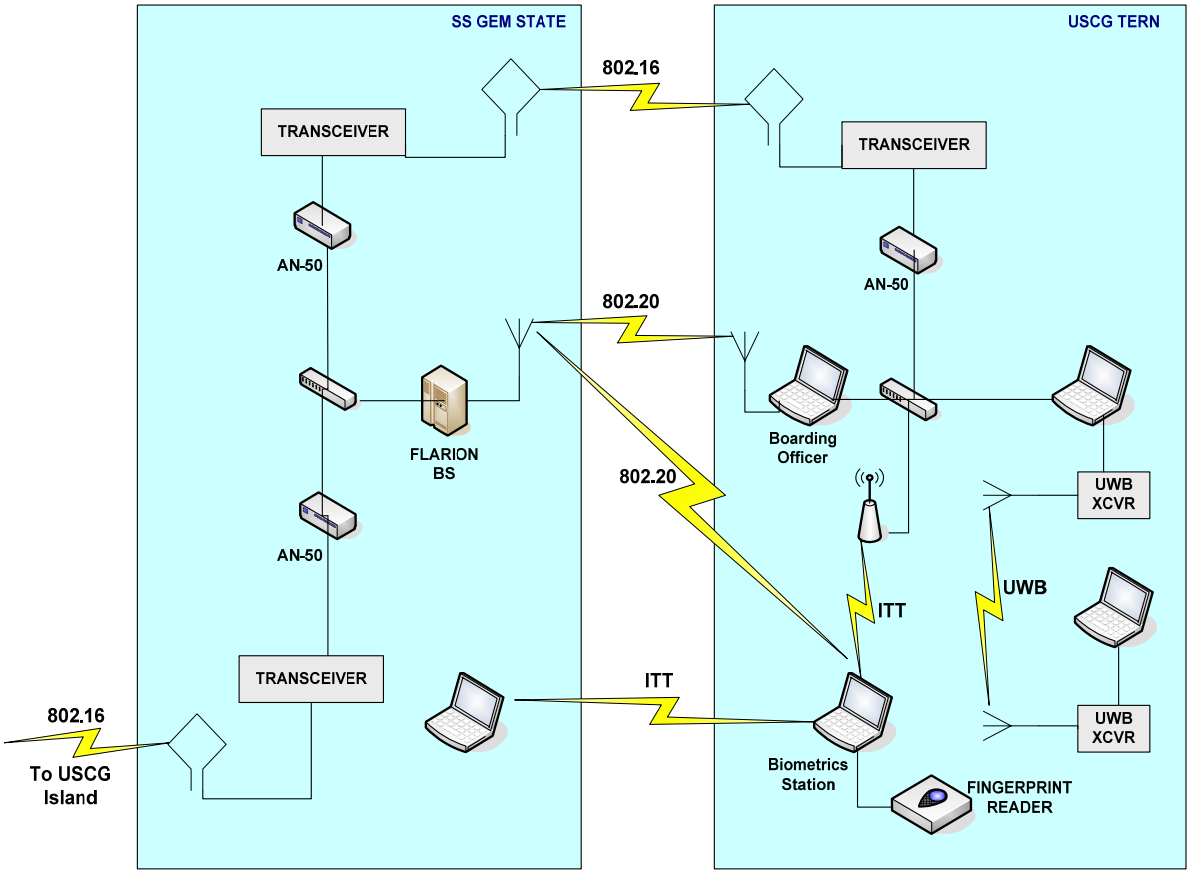

Figure 7. GEM STATE – USCG TERN Network Topology

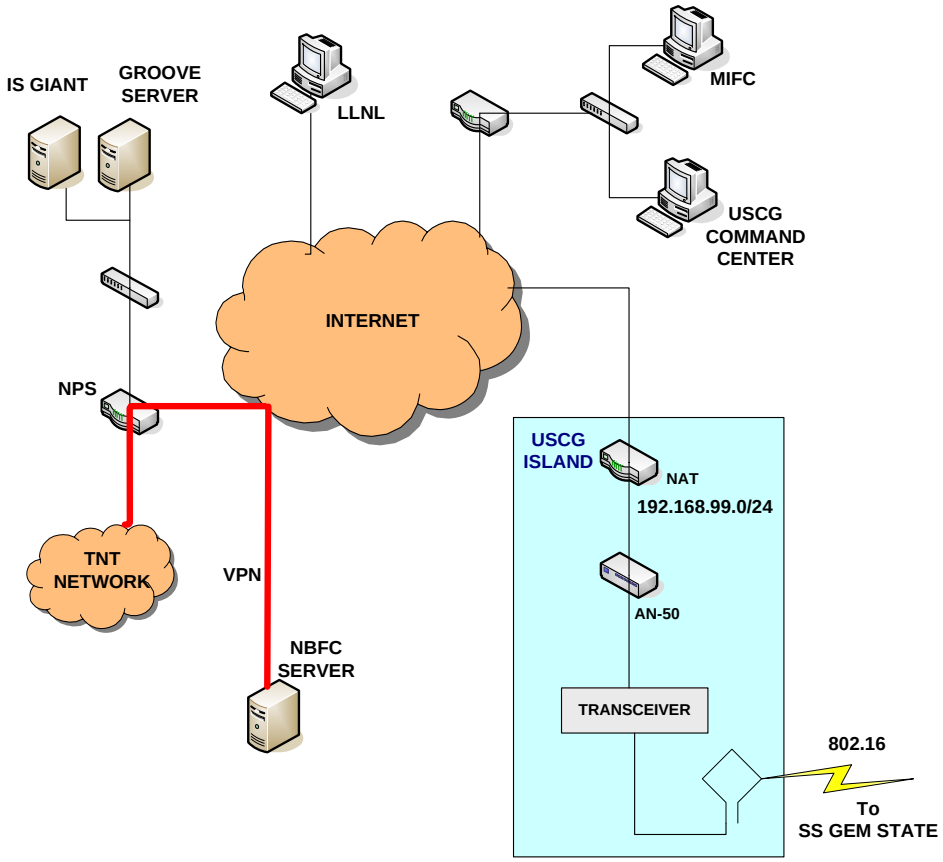

Figure 8. Distributed Centers of Expertise – Operational Command WAN

The Boarding Officer's laptop, as well as the Biometric Station's laptop, was utilized in alternate configurations not depicted in Figure 6: during the transition of the boarding party via the RHIB to the inspected vessel (USCG Tern), the boarding officer's laptop was a node of ITT mesh network in order to test the functionality of sending streaming video back to GEM STATE. While aboard USCG Tern, these laptops alternated between the use 802.20, 802.16 and ITT, being nodes of one or two subnets at a time.

D. SEQUENCE OF EVENTS

During Sunday, March 5, Flarion's FLASH OFDM Base Station along with its 120 degrees antenna was set up on the bridge deck of GEM STATE (Figures 9 and 10). This equipment is not portable and a crane was required in order to haul it up the ship's deck. The wireless PtP 802.16 link between USCG Island and GEM STATE was already set up and aligned the previous week (Figure 11).

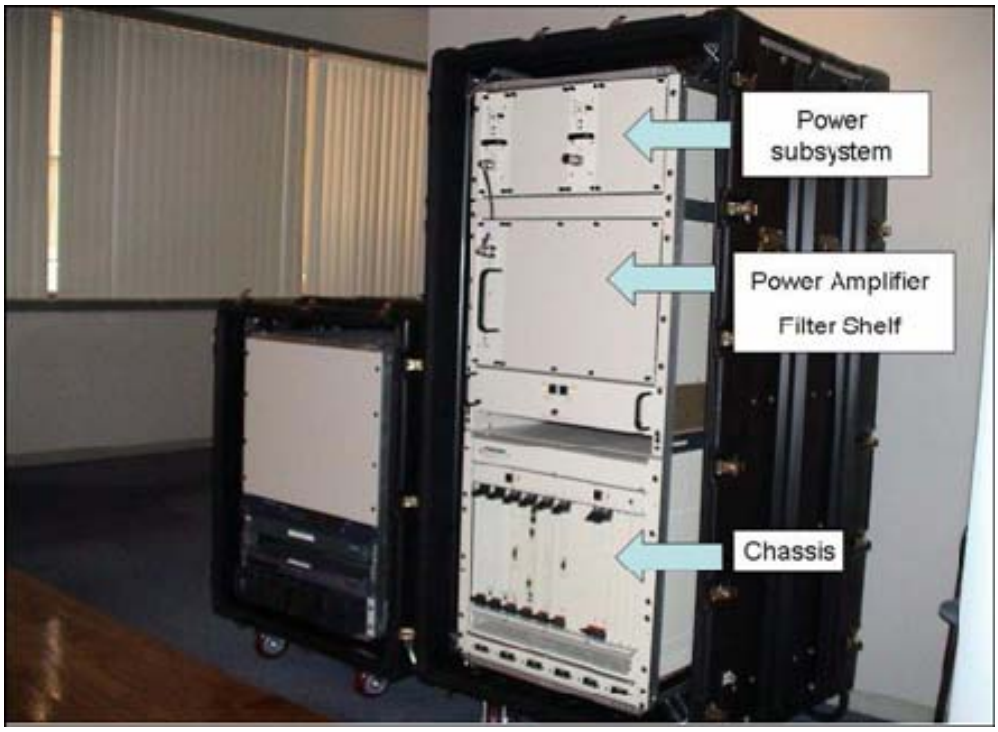

Figure 9. Flarion's 802.20 Base Station (From: Parrish and Tovar, 2005)

Figure 10. Flarion's 120 Degrees Antenna

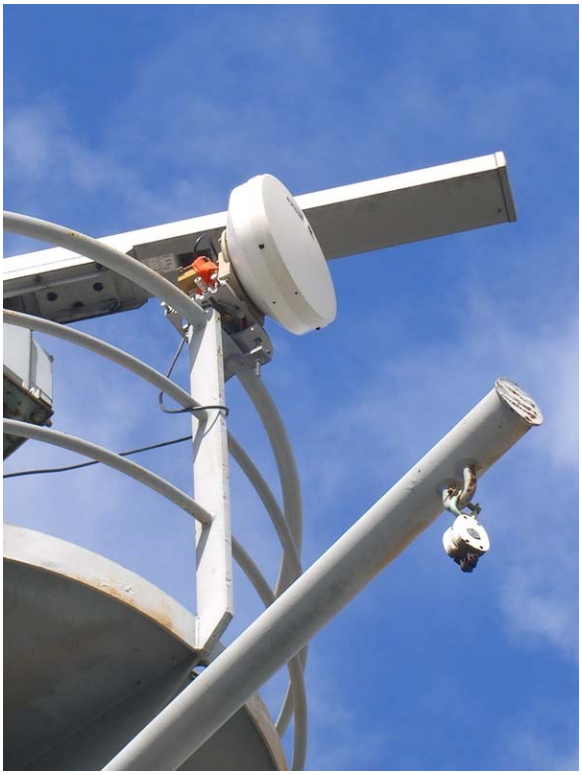

Figure 11. 802.16 Directional Antenna on the Navigation Radar Mast of GEM STATE (GEM STATE – USCG Island 802.16 PtP Link)

Monday morning, March 6, the rest of the network on board GEM STATE was set up, including the TOC, the 802.16 antenna for the GEM STATE-USCG Tern link (Figure 12), and the portable equipment to be carried along to USCG Tern by the boarding party. The Boarding Officer's and Biometrics laptops were equipped with Flarion's FLASH-OFDM Wireless PC Card (Figure 13) in order to become SS of the 802.20 base station.

UWB equipment set up was already conducted on board USCG Tern, since there was a restriction constraining LLNL personnel from boarding a non-docked vessel via vertical ladder. Also, Groove's workspace was established among the experiment participants. At 1450, the boarding team embarked the RHIB in order to transit to USCG Tern. During that transit, adequate quality streaming video was received in Groove's workspace through ITT mesh, as long as there was a clear LOS at a maximum distance of

500 yards. As soon as the boarding party boarded the USCG cutter, the ITT antenna was stripped down aboard the GEM STATE (Figure 14), and another one was set up on board the inspected vessel.

Figure 12. 802.16 Antenna Onboard the GEM STATE (GEM STATE-USCG Tern Link)

Figure 13. Flarion's FLASH-OFDM Wireless PC Card (From: Parrish and Tovar, 2005)

Figure 14. ITT AP Setup Onboard the GEM STATE

During the rest of the experiment on March 6, 802.20 had an outstanding performance, maintaining connection at “near” LOS conditions, while 802.16 again had some issues with the antenna’s alignment. Finally these issues were resolved with manual alignment of the 802.16 antenna on board USCG Tern (Figure 14) achieving a clear LOS (and possibly a clear Fresnel zone).

On Tuesday, March 7, the issues of the previous day had been resolved and the boarding operation commenced at 1028, repeating the same steps as previously. The ship’s navigation radar as well as the 802.20 were shut down in order to check their possible effect on the 802.16 link. As expected, there was no change in the performance of 802.16 link, since the frequency separation between the radar, the 802.16 and 802.20 was great (I-Band/9 GHz, 5.8 GHz, 700 MHz respectively) and the conclusion of the previous day (poor antenna alignment) was verified. Radiation files as well as biometric data files were sent from the boarding party to the respective centers of expertise at an average distance of 1000 yards in order to assist the boarding officer in evaluating the

findings and undertake the right course of action. Finally, a maximum range check was conducted for 802.16, which maintained connectivity at a maximum distance of 2000-2400 yards.

Figure 15. 802.16 Antenna Onboard the USCG Tern

E. EXPERIMENT OUTCOMES – CONCLUSIONS

During the experiment, *Solar Winds Engineer's Edition* network monitoring tool was used by the TOC on board the GEM STATE, in order to monitor the 802.16 link as well as the Boarding Officer's and Biometrics Enrollment laptops. Due to the firewall settings on the 802.20 subnet, it was not possible to monitor with SNMP or even ICMP that subnet from the TOC. Furthermore, due to NAT setting on the USCG Island router, it was not possible for the NOC at NPS to monitor and gather data remotely, so all the network monitoring had to be performed locally by the TOC. Another problem was that the Redline's MIB's are not yet compliant with the Solar Winds MIB Browser Tool, and therefore the monitoring of the 802.16 links was enabled only by ICMP, providing only packet loss and response time (latency).

In addition to Solar Winds, Redline's *RF link monitoring tool* was used in order to monitor the 802.16 link, providing real time values of the Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR). This tool was mainly used in order to point out the existence of RF interference and the bad alignment of the 802.16 directional antennas, and trigger the boarding party to correct these issues manually.

Finally, since the monitoring of the 802.20 subnet was not possible through Solar Winds, it was performed by Flarion's *Mobile Diagnostic Monitor* (FMDM). That software tool is used for gathering data during drive testing, and exports the collected data into XML files. It is typically loaded on a laptop PC equipped with both a mobile PCI card for communicating with the Base Station, and a GPS device for capturing positional and time information. During the experiment, it was installed on the boarding officer's and biometrics enrollment laptops, which were equipped with the Flarion's PCI cards, but not with GPS devices, resulting in no data about the time or the position of these SS's.

Considering the USCG Island – GEM STATE (ship-to-shore) 802.16 link first, no trouble at all was encountered there, since the GEM STATE was docked, and the link was actually a fixed PtP link. The precise alignment of the antennas had been performed prior to the execution of the field trial, and both the packet loss and the response time were minimal, as illustrated in the following figures.

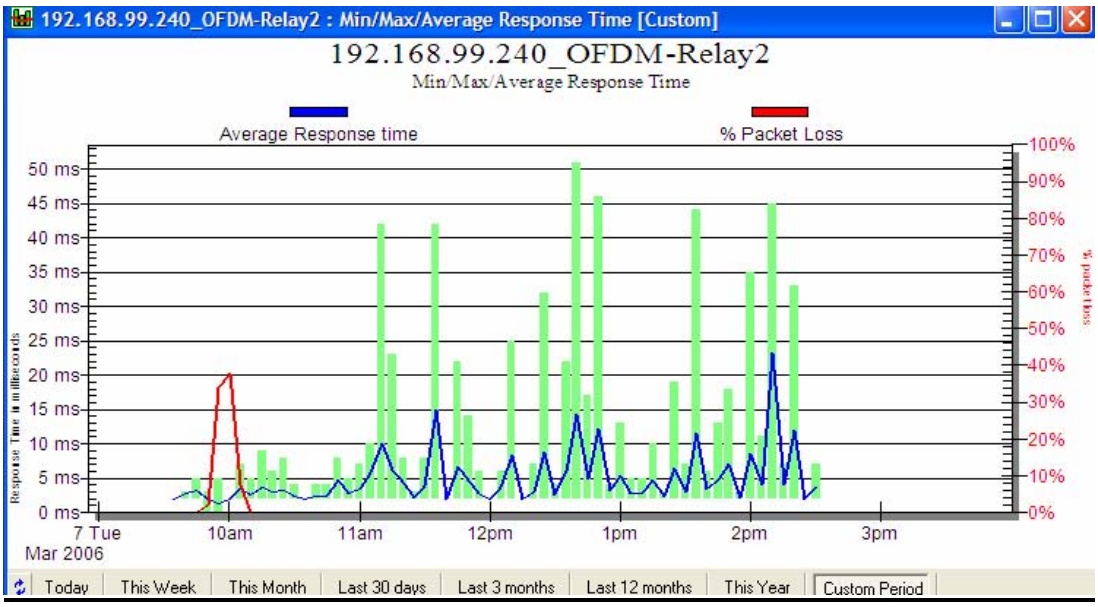

Figure 16. GEM STATE – USCG Island 802.16 Link Response Time and Packet Loss (on USCG Island)

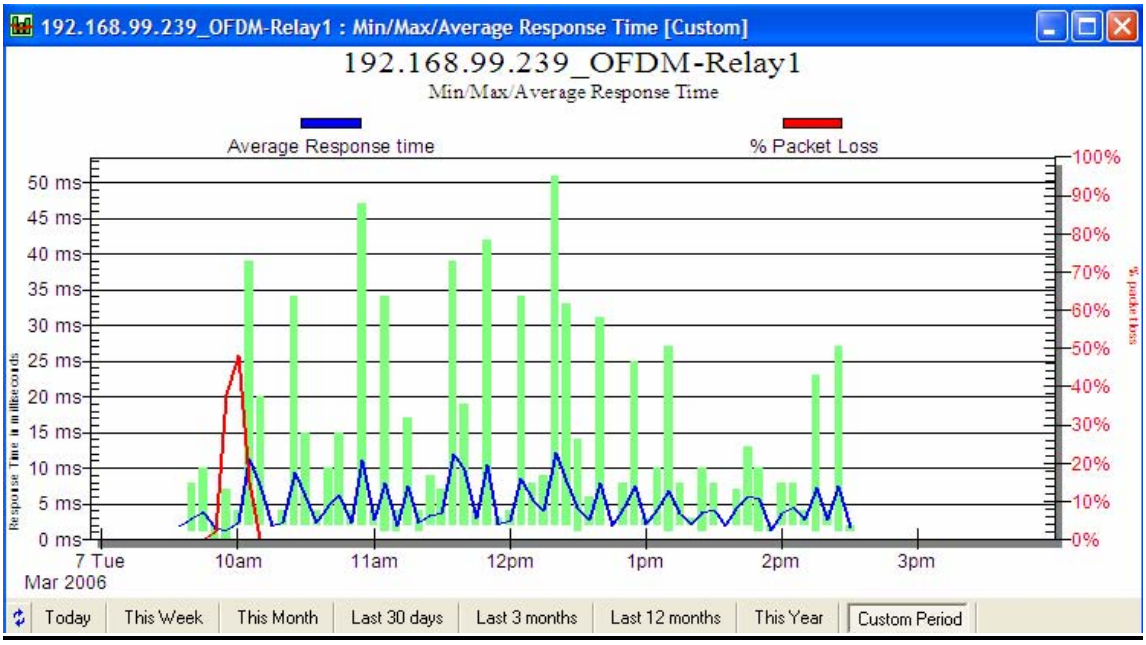

Figure 17. GEM STATE – USCG Island 802.16 Link Response Time and Packet Loss (on GEM STATE)

On the other hand, the GEM STATE – USCG TERN 802.16 link, experienced some issues concerned only with the antenna alignment. Since the target vessel was underway, the antenna was not omni and was mounted on its stern pointing aft, there were numerous times when there was no LOS at all. Choosing a directional antenna in order to increase the link budget and support higher data rates, resulted in periods when the link was down (Figure 18); in response, a boarding party member had to visually aim the antenna towards the GEM STATE, while the target vessel had to steer accordingly. When the LOS was getting re-established, the 802.16 link was able to maintain an excellent connection; at an average distance of 1000 yards with an RSSI of 60 dBm and an SNR of 12 to 15 dB, the packet loss and response time were minimal, and the link could adequately support the boarding party's data exchange needs, including streaming video application from the target vessel. The overall performance of the support vessel-target vessel 802.16 link is illustrated in Figures 19 and 20. The link was finally tested successfully up to 2400 yards, while there were no conclusions on the effects of the target mobility. Overall, the only visible problem on the subject was the aforementioned, and is expected to be solved with the acquisition of self aligning antennas. Another subject for future consideration should also be the relative movement of the 802.16 nodes, since the IEEE 802.16e mobility standard is still pending.

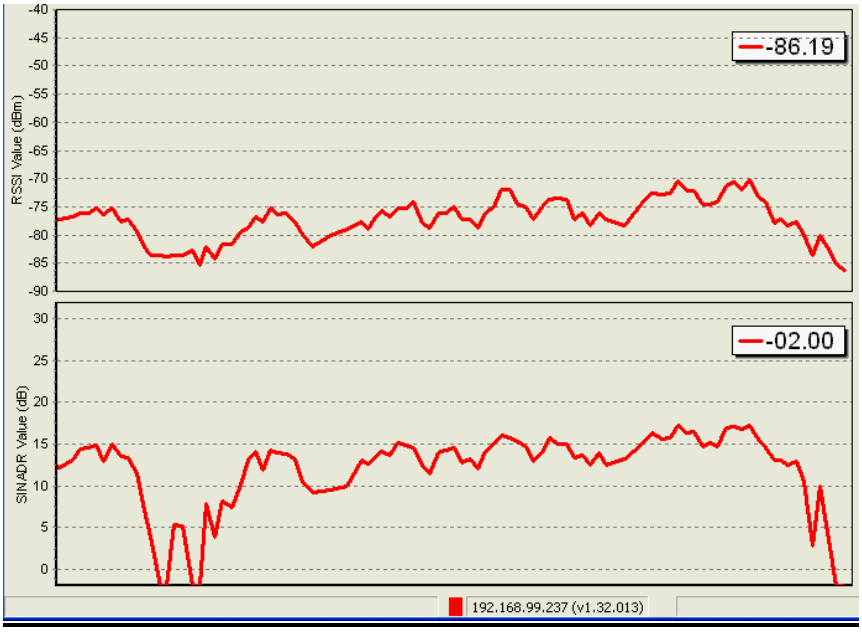

Figure 18. RSSI & SNR for the GEM STATE – USCG Tern 802.16 Link at 11:20 (Link Down Due to NLOS)

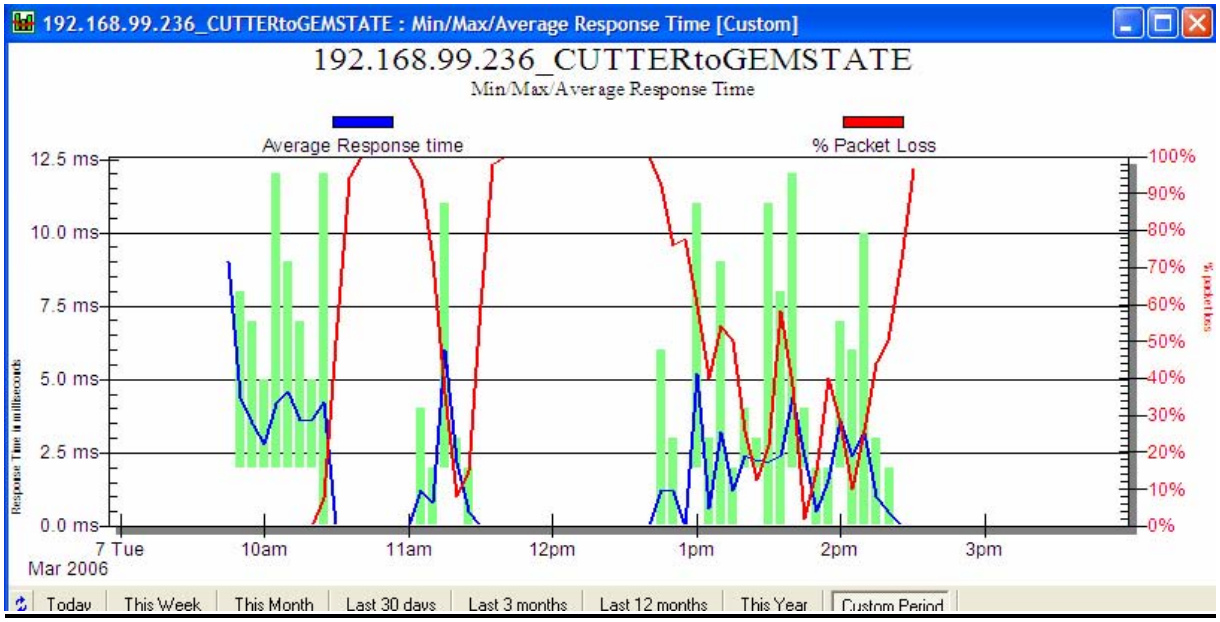

Figure 19. Latency and Packet Loss for the GEM STATE – USCG TERN 802.16 Link (on USCG TERN): Peaks in the Two Variables Correspond to NLOS Conditions

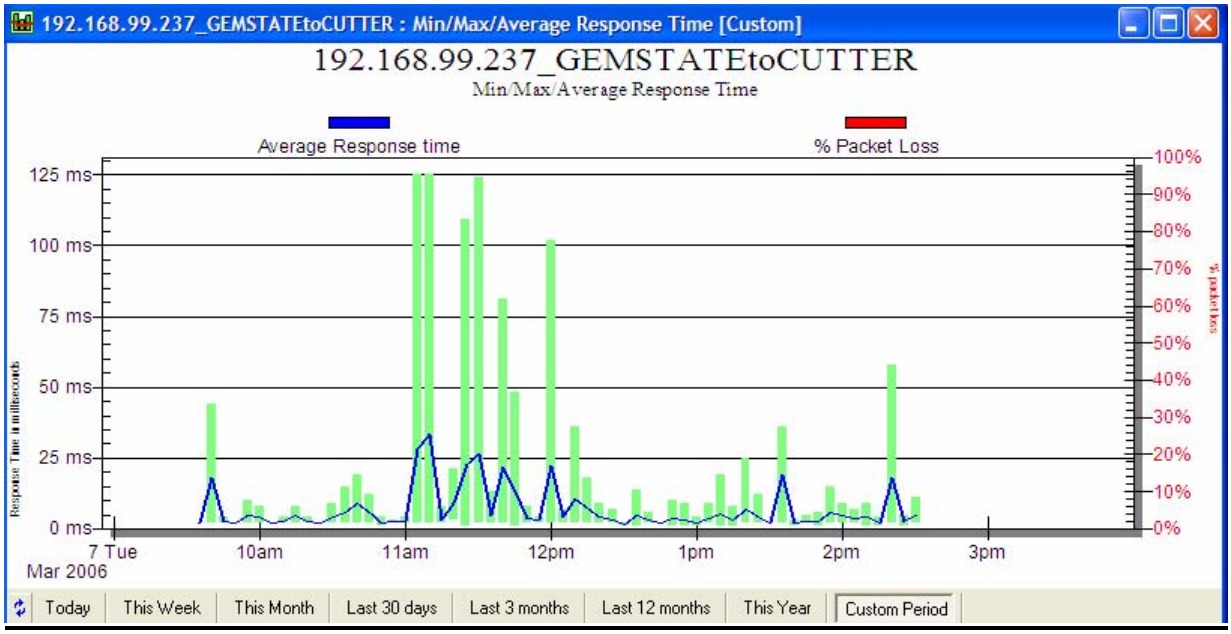

Figure 20. Latency and Packet Loss for the GEM STATE – USCG TERN 802.16 Link (on GEM STATE)

Monitoring the performance of the Ethernet interface of the boarding officer's laptop (connected to the Redline's AN-50 through the switch) was possible with SNMP / Solar Winds. That gave us an indication of the collaboration traffic (Groove transactions) going through that interface, as illustrated in the following figures.

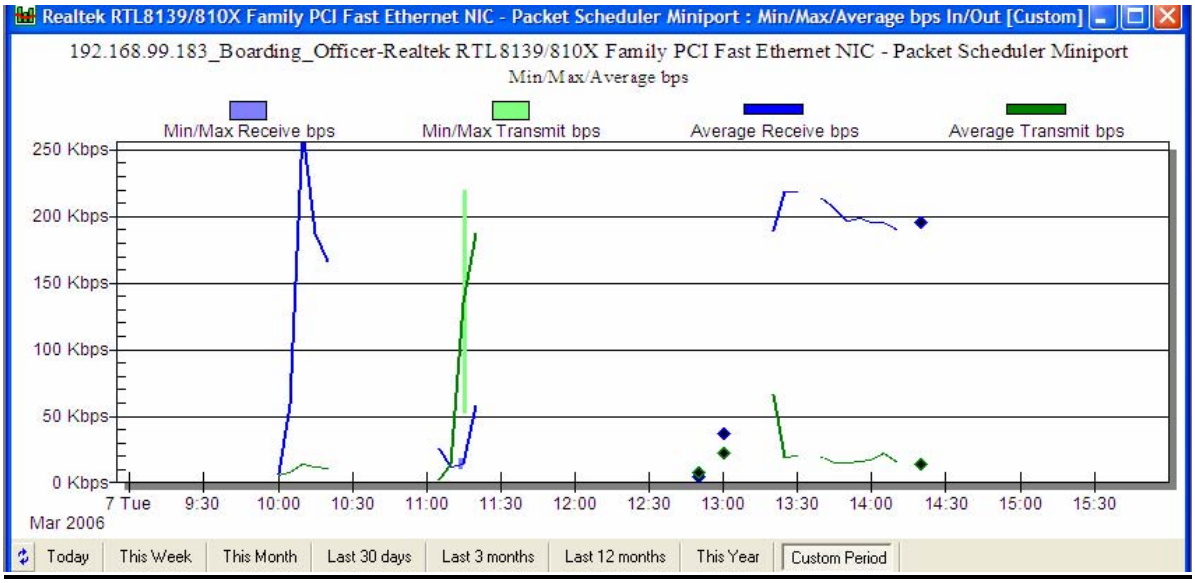

Figure 21. Boarding Officer's Laptop Ethernet Interface: In/Out bps

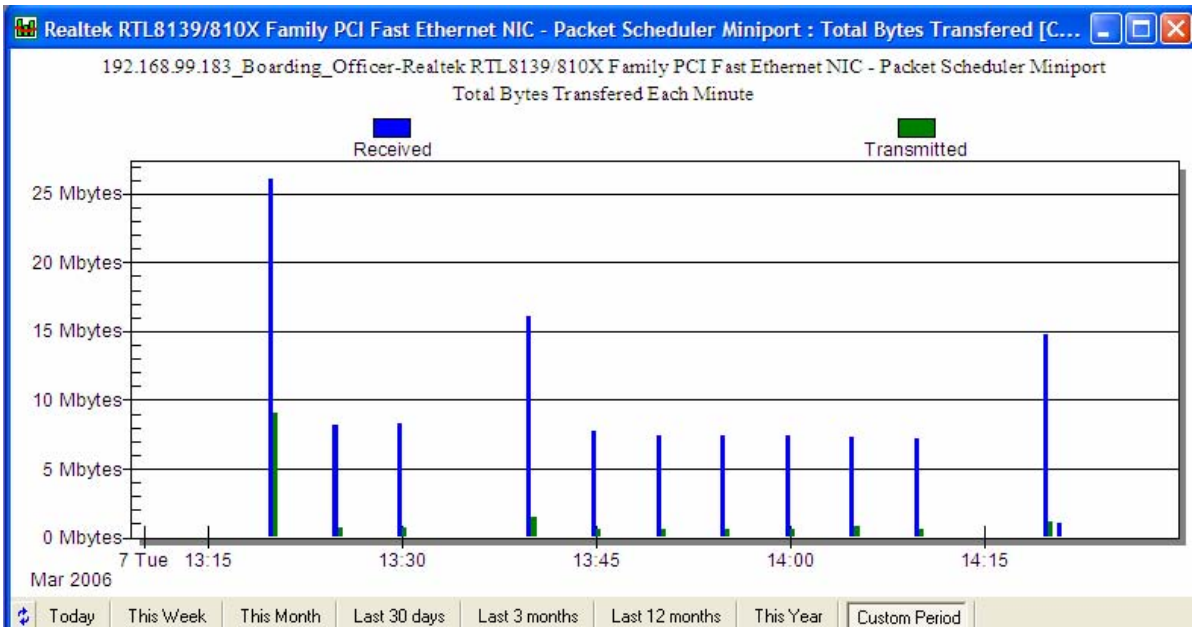

Figure 22. Boarding Officer's Laptop Ethernet Interface: ifInOctets / ifOutOctets

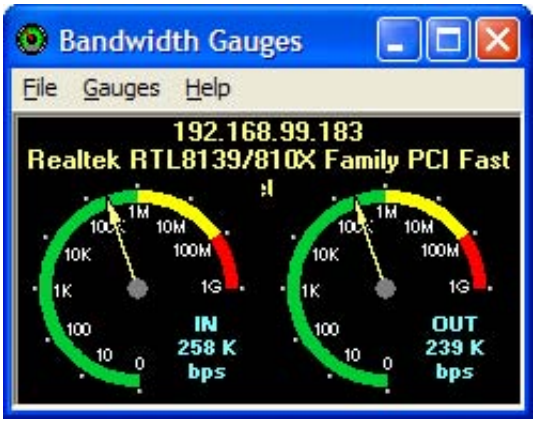

Figure 23. Boarding Officer's Bandwidth Gauge at 1318, March 7

That indication though did not include all the collaboration transactions taking place on the boarding officer's laptop. Since both the wireless (Flarion's PCI card) and the wired (Ethernet to AN-50e) interface were used simultaneously, it was not possible to tell whether the traffic was going through the one or the other. Although, the packets followed one of the two routes, that variation of the physical and link layers was transparent to the application layer, which indicated a continuous connection and collaboration between the boarding officer and the rest of the nodes of the TNT expanded network external to the target vessel.

The same principle applies for the biometrics enrollment station as well. It was a node of more than one subnet at the same time: 802.16 via the wired (Ethernet) and ITT or 802.20 via the wireless interface. The next two figures, obtained from Flarion's *Mobile Diagnostic Monitor* (FMDM) raw data files (XML) converted to scatter plots with the use of Excel, indicate a maximum downlink (DL) throughput of approximately 1.5 Mbps for the 802.20 base station-biometrics laptop link. Lack of GPS data on the biometrics laptop did not allow for correlation of the distance with the throughput.

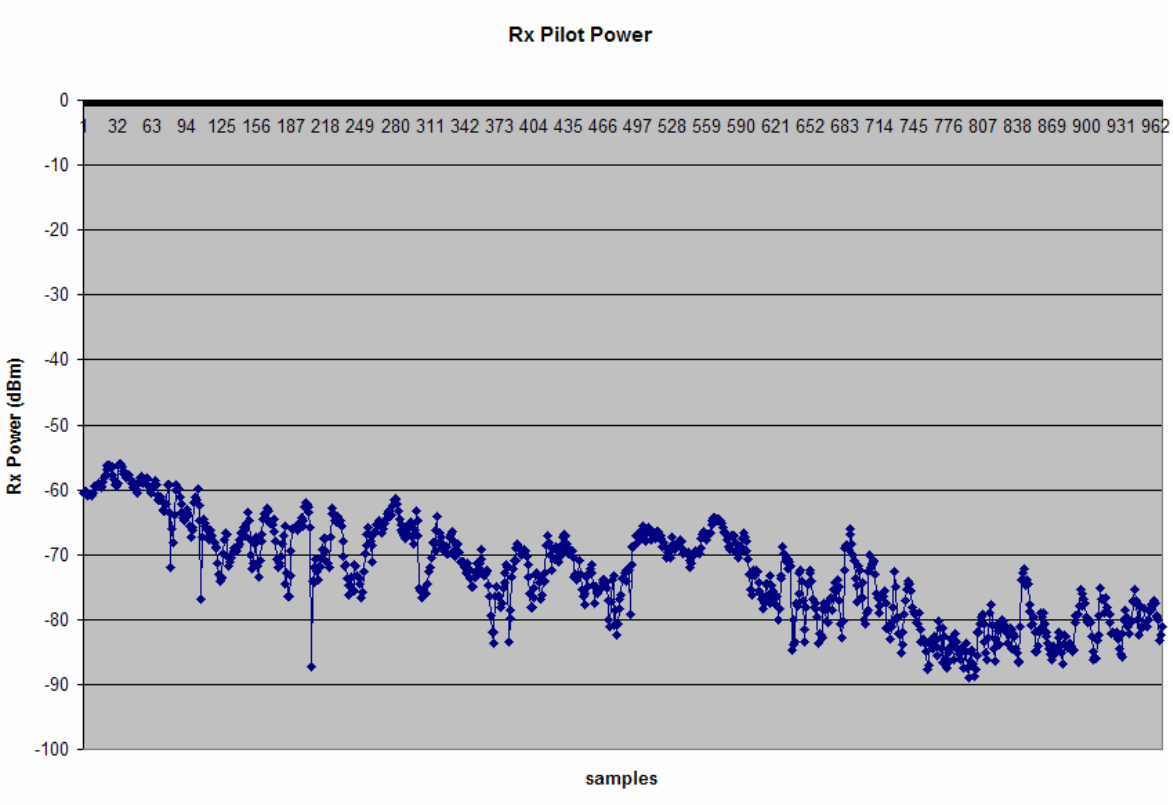

Figure 24. Biometrics Laptop (March 7): Rx Pilot Power (dBm)

The above figure gives us the received signal power in dBm, for each obtained sample, on the laptop's PCI card from the base station (Active Rx Pilot power). The following figure converts the Active Rx Pilot Power from dBm to SNR, and afterwards displays the bit rate as a function of the SNR:

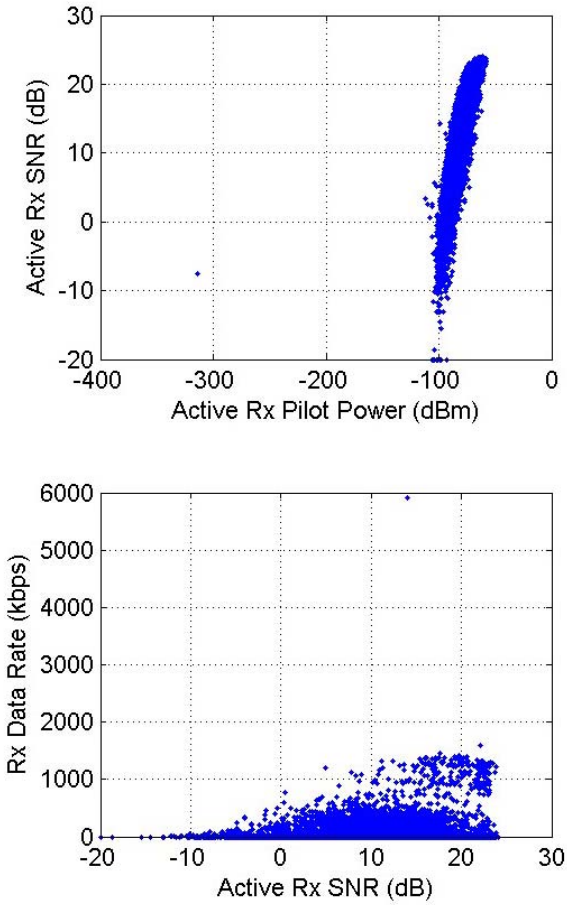

Figure 25. Active Rx Pilot Power: Conversion from dBm to SNR, and DL Throughput Display as a Function of SNR

Overall, the performance of 802.20 proved to be exceptional for distances from the base station up to 3 nm and near LOS conditions, compared to the 2400 yards obtained from the 802.16 link (Figure 26). Although PCI cards were used on the SS's instead of external antennas, the range superiority of 802.20 can be attributed to the lower utilized frequency (700 MHz) and thus to better propagation characteristics, the higher output power (20 W), and the wider lobe antenna (120 degrees). There was no testing on the SS speed or the number of SS's that can be accommodated by the base station without saturating the link.

Figure 26. Max Link Connection Ranges - Map of the Experiment Site

The ITT mesh network performed well, being able to provide a wireless link between the boarding officer and the TOC onboard the GEM STATE, while the boarding party was transiting to the target vessel via the RHIB; streaming video from the RHIB was sent during that transit up to a distance of 500 yards. Once the boarding party boarded the target vessel and set up the ITT access point there, it was not possible to maintain connection with the mesh node onboard the GEM STATE at ranges of 500 yards or greater.

The UWB wireless LAN on board the target vessel performed reliably (Figure 27) as expected, providing radiation material pictures and video from the internal spaces of the vessel. TNT 06-2 field trial was not a challenge for that technology, since the target vessel had a much smaller hull than the target vessel of the TNT 06-01 experiment.

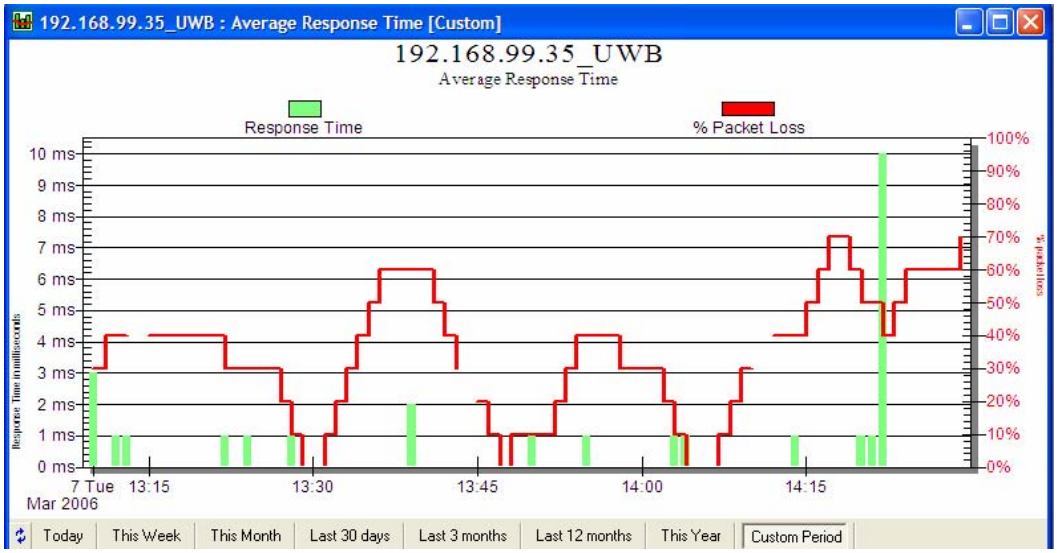

Figure 27. UWB Link Latency and Packet Loss

For the collaboration needs of the participants, one workspace in Microsoft's Groove was used (Figure 28), which provided the boarding officer with the necessary situational awareness in order to make the right decisions, depending on the evaluation of his findings by the remotely located experts. Additionally, video stream from one or more cameras / links was another application that provided the remote collaborators / nodes, with a clear picture of the boarding progress (Figure 29).

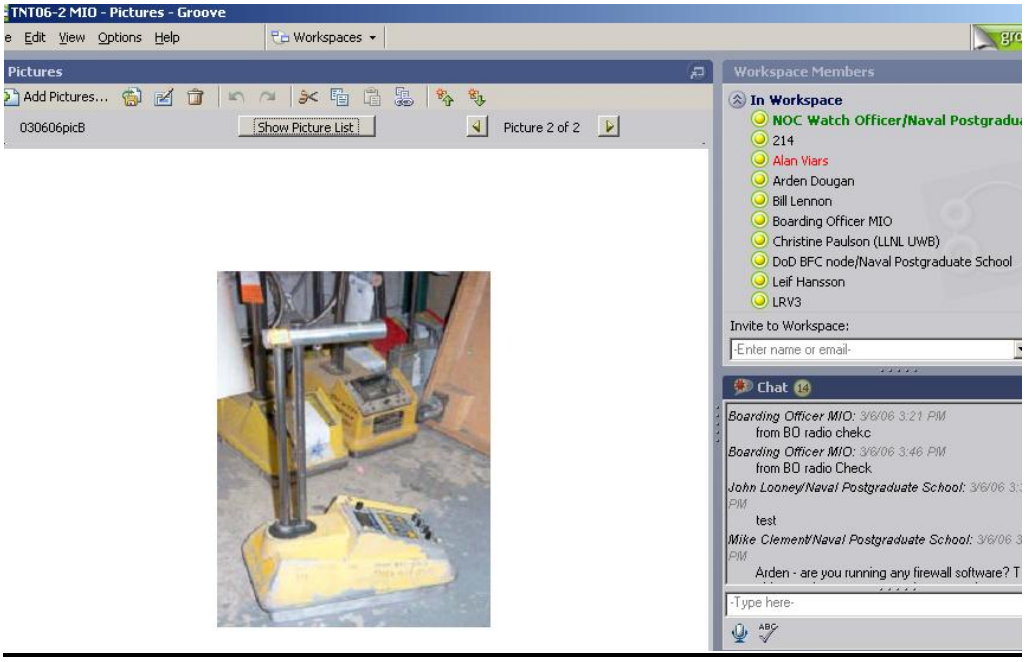

Figure 28. Groove Collaborative Tool Utilization

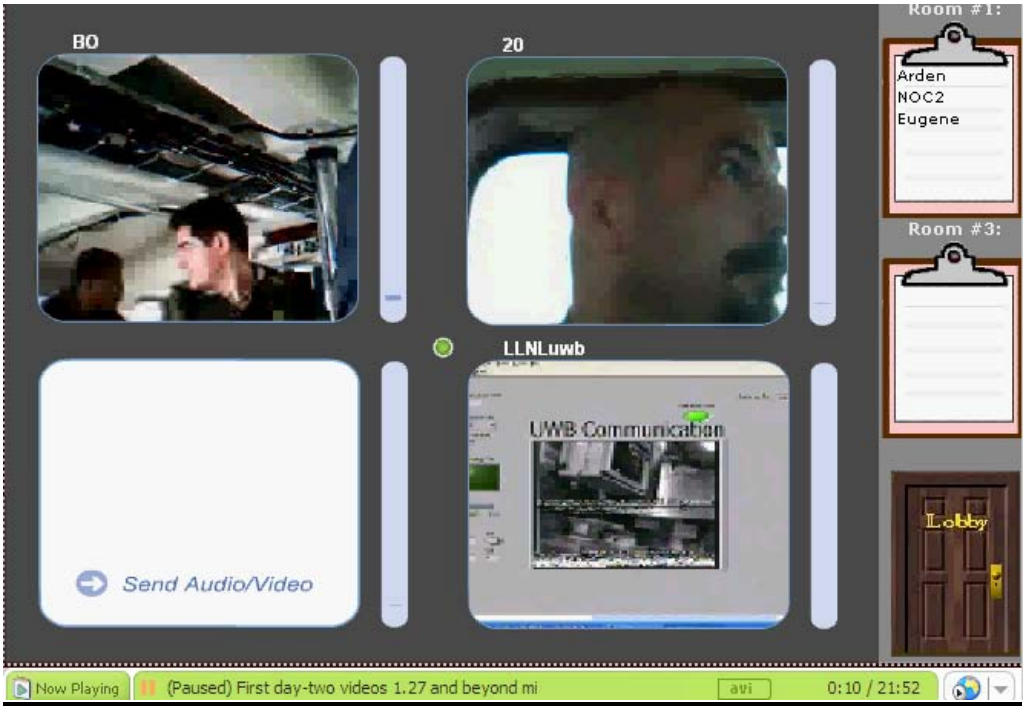

Figure 29. Streaming Video through the 802.16-802.20 Links at a Distance of 2400 Yards

V. TNT 06-3 FIELD TRIAL

A. EXPERIMENT SCENARIO

The scenario of TNT 06-3 experiment for Maritime Interdiction Operations was somewhat differentiated from TNT 06-2: since UWB and ITT wireless technologies had already been tested successfully in past experiments along with IEEE 802.16 and 802.20, the focus of TNT 06-3 was on the situational awareness and correct decision making capability created by the participants and collaborative tools employed during a more sophisticated scenario than the previous ones. Although the technologies and the collaboration tools did not change from the previous field trials, more players were added into the collaboration environment of TNT 06-3, increasing the complexity of interactions as well as the workload of the boarding officer. Overall, the sequence of events according to the experiment scenario was the following:

1. Intelligence and Events from Foreign Collaborative Partners

An Austrian border control has detected a radiation source on a truck, but due to a detection equipment malfunction, the truck was not searched and was allowed to continue its transit. Further intelligence provided the piece of information that the truck might have unloaded its cargo onto a ship, under Swedish registry, in a Baltic Sea port. The Swedish authorities are conducting boardings trying to locate the radiation source without any luck so far. The ship that the truck's cargo has probably been loaded on, is still unknown and can be anywhere in the world at this time.

2. San Francisco Bay Events

While on routine patrol in San Francisco Bay, SFPD Marine Unit-3 RHIB (Figure 30), equipped with radiation detection sensors, receives a radiation alarm as it cruises past a fishing boat (simulated by Alameda County Sheriff's Marine Patrol Boat) (Figure 31). The alarm is initially reported to RAP (Radiation Assessment Program, in this case simulated by LLNL) by the skipper of SFPD Marine Unit-3, using voice communications, and subsequently to USCG District 11, to which, the radiation data files obtained from the sensors are sent for investigation, using a wireless data link. MIFC is invited to join the collaboration environment as well, in order to provide a background check on the suspect vessel and additional related intelligence on radiation materials

smuggling. At that point, the issue of the radiation source that has been recently detected in Austria surfaces, remotely bringing into the collaboration both Austrian and Swedish authorities, in order to investigate the possibility of having radiation material transported from Austria to the Baltic Sea with the final destination being the San Francisco Bay area.

Figure 30. SFPD Marine Unit-3 RHIB (Initial Radiation Detection) (After: Bordetsky, 2006)

Figure 31. Alameda County Sheriff Marine Patrol Boat (Suspect Vessel)

An MSST (Maritime Safety and Security Team) is sent under the authority of District 11, in order to conduct a Level 2 search of the suspect fishing boat. After they transit via the Alameda County Sheriff RHIB (Figure 32) to the suspect vessel and secure it, they set up a wireless network extension from the sea to shore in order to join the collaboration environment. Once connectivity is established, SFPD Marine Unit-3 is dismissed from the scene of action by the boarding officer. Then, the MSST team proceeds with the search boarding process, which includes scanning for radiation indications with Identifinders and taking biometric samples from the crew members. At that point, NBFC comes into play in order to cross examine the received fingerprint samples with their database for a possible hit for suspects on the watch list.

Figure 32. Alameda County Sheriff RHIB (MSST Transport) (After: Bordetsky, 2006)

Under the aforementioned course of action, an exchange of information commences between the boarding officer, the collaborating centers of expertise (LLNL, NBFC), the operational command (District 11) and the sources of intelligence (MIFC, Austrian and Swedish authorities). Utilizing various Groove workspaces, a common, synchronized situational awareness is built among the collaborators by exchanging information in several formats: radiation spectrum and fingerprint data files, streaming video, pictures, and text messages containing boarding situation reports, analysis and feedback on the findings on board the suspect vessel and clarifications on what is going on during the boarding. The ultimate goals of the collaboration are to determine:

- The sources of the radiation initially detected by the SFPD Marine Unit-3 RHIB
- If there are any crew members of the suspect vessel on the terrorist watch list
- If the radiation sources are related to the Austria-Sweden incident
- The search hazards for the MSST team, and the initial risk assessment for the area associated with the discovered radiation materials
- The appropriate course of action depending on all of the above

B. EXPERIMENT OBJECTIVES

TNT 06-3 experiment's objectives were augmented in comparison to the previous TNT MIO field trials: in addition to the technical issues of the experiment, the

operational aspect was tested more thoroughly this time, in order to explore ways of adjusting the successfully tried technology, to military and law enforcement, real world operating procedures and vice-versa.

1. Operational Objectives

The primary objectives of the TNT 06-3 field experiment were the operational issues that arise with the use of newly introduced technology, tools and capabilities in the execution of MIO's. In overview, TNT's experimentation is one of the many successive DoD steps towards NCW (Network Centric Warfare). NCW though, is not just about connecting far away nodes. Alberts et al., (1999, 3) highlight the fact that performance advantages from the adoption of new technologies lead to the emergence of new doctrines, tactics, techniques and procedures; command and control concepts need to change in order to take full advantage of the technology. Therefore, the advances in technology move side by side with the concept of operations, which has to be rediscovered. The main objective then, of TNT 06-3, was to discover that new concept of operations that has to be implemented in Maritime Interdiction Operations and Communications. In order to do that, insight must be provided to several related issues, such as:

- The capability of the utilized collaborative applications (Groove, SA, E-Wall) of providing to all nodes a common, synchronized operational picture and situational awareness.
- The amount of the required information sharing between the numerous sources dispersed in several locations worldwide, in terms of bandwidth, and messaging frequency.
- The format of the information that has to be exchanged, in terms of type (data files, streaming video, photographs, text messages, etc), standardized language, clarity, brevity, and common understanding between users with different educational background, and native language.
- The timeliness of the exchanged information, not just in terms of network delay, but moreover in the time required for processing and analysis of the received data, for correlation and consolidation with other pieces of information and production of an output that is useful for the other nodes.
- The development of standard operating procedures (SOP's) for MIO's boardings that reflect the new capabilities of the network-centric environment.

- The nodes that the network must incorporate, either because they possess the necessary expertise and information, or the administrative rights and authority, in order to successfully accomplish all possible scenarios of MIO missions. For that reason, among the collaborators in TNT 06-3, were additional organizations of the law enforcement community as well as international agencies.

2. Technical Objectives

Once again, the technical issues to be investigated included:

- Checking for potential hardware / software problems and limitations in establishing the ship-to-shore and within the ship wireless networks. The UWB technology was not tested again in this experiment.
- Investigation of the reliability and performance of the utilized wireless networks in accordance with the information exchange requirements in terms of range, throughput, latency, and packet loss.

The ability of the boarding party to rapidly set-up the necessary networks was not tested again, since previous TNT MIO field trials repeatedly proved that the time required for that was acceptable (15-20 minutes).

C. NETWORK TOPOLOGY

During the TNT 06-3 experiment, the part of the collaborative network that was extended to sea to the assisting vessels and the boarding party, is displayed in the following figure:

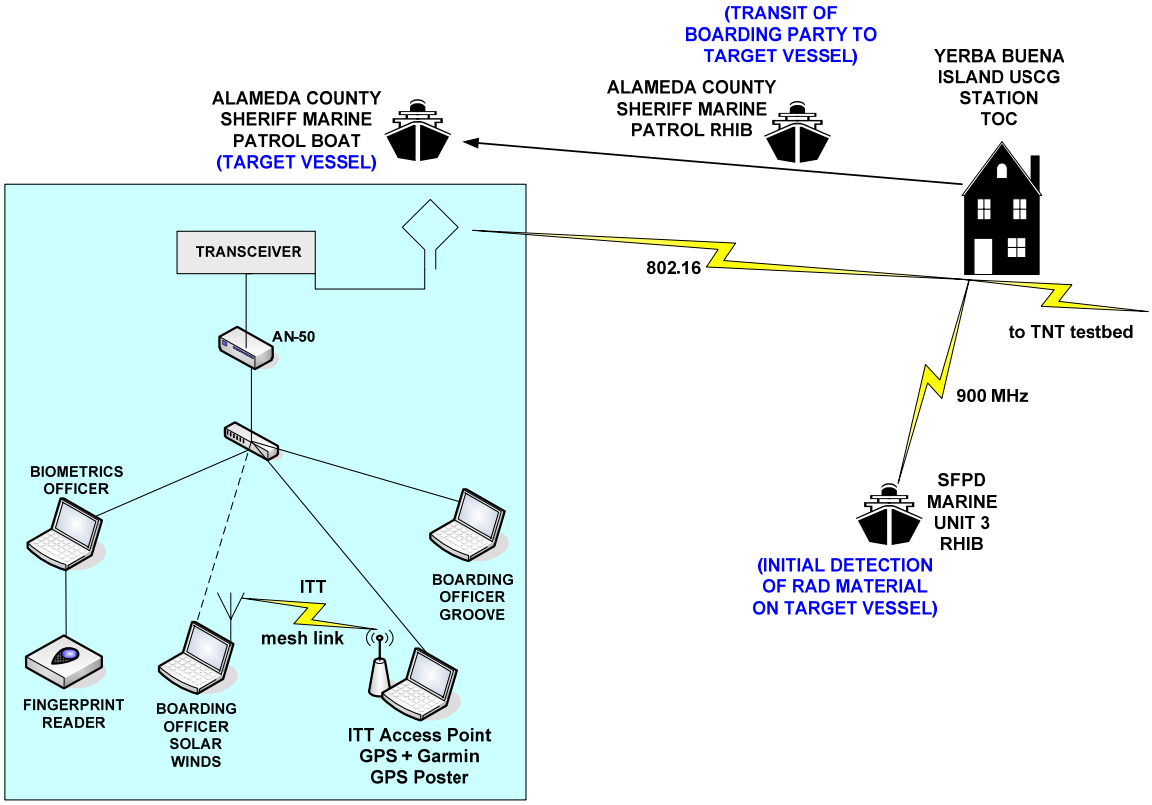

Figure 33. TNT 06-3 Network Extension to Sea

The TNT testbed network extended the collaborative environment from the San Francisco bay area up to the NPS / CENETIX lab, LLNL, the Austrian and Swedish counterparts, and District 11 command and control facilities:

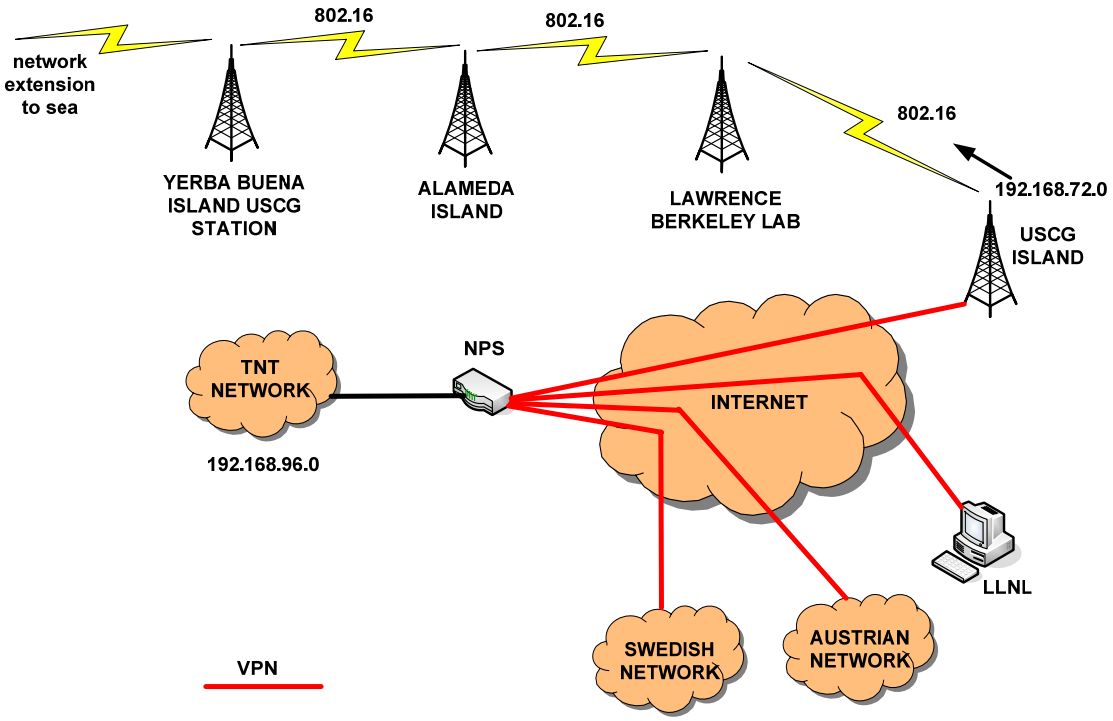

Figure 34. TNT 06-3 Testbed

D. SEQUENCE OF NETWORK INTEGRATION AND OPERATION EVENTS

1. Monday, June 12

The first day of the field trial was a set up day for both the TNT TOC at Engineering Building 1 in USCG Station of Yerba Buena Island and the target vessel. The portability of the boarding party equipment had been proven in the previous MIO experiments and since there were no changes in the utilized hardware / software, it was decided to set up the network on Alameda County Sheriff Marine Patrol boat (suspect vessel) in advance. Instead of the AN-50's, AN-80's were used initially as wireless bridges in order to connect the target vessel and the TOC via the 802.16 link, but for unknown reasons, one of the two devices was unable to be configured through the Redline GUI, and therefore the AN-80's were replaced with the AN-50's the following morning.

In detail the set up onboard the target vessel included:

- Setting the 802.16 directional antenna (Figure 35) on a machine gun mount so that it could rotate on the horizontal level towards the antenna on the roof of the TOC building.

- Connecting the antenna to the transceiver via the RF cable and the transceiver to the AN-50.
- Connecting the AN-50 and the two Pelco camera video devices to the network switch as well as the laptops needed for accomplishing the tasks of the boarding party (Figure 36): one for monitoring the network (equipped with Solar Winds), which was also a node in the mesh ITT network, one for interacting in the collaboration environment (equipped with Groove) and one for recording and sending the location (latitude / longitude) of the target ship to the shore (equipped with GPS receiver and poster), which was also the access point for the ITT mesh network. The Biometrics Enrollment laptop was not setup until the next day.
- Setting the ITT mesh network between the GPS laptop (access point) and Solar Winds laptop. No other mesh nodes were used during this field trial.

As described previously at the experiment scenario, the initial detection of radiation was conducted by SFPD Marine Unit-3 RHIB sensors. In order to report that, as well as to provide radiation data files to higher authorities for further investigation, a 900 MHz link was established between the TNT TOC at Yerba Buena Island USCG Station and that RHIB. That allowed the radiation detection personnel on board the RHIB to join the relevant Groove workspace and exchange information with RAP authorities (LLNL).

The second wireless link was established between the suspect vessel (Alameda County Sheriff Marine Patrol Boat) and the TOC. That link provided connectivity of the boarding party with the rest of the nodes in the collaborative environment. In addition, a mesh network was set up between two laptops onboard the suspect vessel, providing wireless connectivity to the Boarding Officer's network monitoring laptop to the rest of the network.

Figure 35. 802.16 Link Directional Antenna Onboard the Target Vessel (After: Bordetsky, 2006)

Figure 36. Suspect Vessel NOC Laptops (From Left to Right: Network Monitoring / SolarWinds, Collaboration / Groove, ITT Mesh Access Point / GPS Receiver-Poster)

2. Tuesday, June 13

The second day of the field trial was a test day, in order to find out and fix the discrepancies before the actual execution of the experiment's scenario the next day. Initially, the 900 MHz wireless link (Figure 37) was setup on SFPD Marine Unit-3 RHIB, to provide the data link with the TOC (reliable connectivity was possible only under LOS

conditions though). At 1230, the experiment commenced, with the RHIB passing at the proximity of the target vessel. The radiation from the sources was picked up by the sensors on the RHIB, and after notification of LLNL and District 11 through Groove, the MSST party boarded the suspect vessel at 1313.

Figure 37. 900 MHz Antenna Onboard SFPD Marine Unit-3 RHIB

During the boarding search, three radiation sources were discovered by MSST's Identifinders and were reported via Groove chat to District 11 using the target vessel's laptop. Two of them were previously hidden by LLNL personnel for the scenario purposes, while the third one was an old smoke detector. The obtained radiation data files of the above sources were transferred from the Identifinders to the LLNL laptop and from there to the boarding party's Groove laptop via flash memory stick, in order to be posted in the Groove's workspace. That way, all files were successfully received and opened for analysis and evaluation by LLNL reachback.

Additionally, three sets of fingerprints were also sent from the Biometrics Enrollment laptop, on board the suspect vessel, to the Biometrics Master computer, at the USCG Station TOC. The responses from the Biometrics Master computer came back

negative with no hit in the database, two minutes after the submission of each fingerprint data file. Because the Biometrics Enrollment laptop was not loaded with Groove's client software, a flash memory stick had to be used again, in order to transfer these files from the Biometrics Enrollment laptop to the boarding party laptop, and post them in Groove.

At 1413, the MSST completed the search of the target vessel, and at 1445 the experiment was concluded. Although a connectivity problem was never encountered between the suspect vessel and the TOC, and all traffic from the boarding party was successfully received by the relevant collaborators in Groove, some of the issues that emerged the first day of the experiment were:

- Incorrect time stamps on several Groove's client laptops. Internet time, or CENETIX lab server GPS time had to be set on all Groove laptops.
- Connectivity problems through the backbone wireless link between the TOC and Berkeley (perhaps, due to construction on the San Francisco Bay Bridge, obscuring the LOS / Fresnel Zone).
- Wrong use of Groove's workspaces. In contrast to the past TNT MIO experiments, instead of just one workspace, three Groove's workspaces were established and used in TNT 06-3, getting closer to reality, but also increasing the communications complexity. These workspaces were the following:
    - District 11 workspace, for command, control and decision making
    - Boarding Party workspace, concerning findings onboard the suspect vessel and their analysis results
    - Network workspace, for technical issues and experiment control

Posting of files or chatting on the wrong workspace deprives required information from some users, while overloads others with information they do not need.

3. Wednesday, June 14

The third day of the field trial was the actual MIO scenario execution. Again, the beginning of the experiment commenced with SFPD Marine Unit-3 RHIB cruising at the proximity of the suspect vessel. The planted sources of radiation were detected by the LLNL radiation sensors onboard the RHIB at 1120, and were reported via the 900 MHz data link / Groove to RAP (LLNL). The obtained radiation data files were also posted on Groove and received by LLNL for analysis and recommendations on the appropriate course of action. The target vessel was detained by SFPD Marine Unit-3 RHIB and upon

notification of District 11, the MSST was authorized and executed the boarding at 1214. Shortly after that, the SFPD Marine Unit-3 was relieved from the scene of action by the boarding officer.

The boarding party replaced the directional antenna of the 802.16 link with an omni antenna (Figure 38) in order to avoid having someone continuously pointing the antenna towards the TOC antenna as the boat was moving around, while a new laptop was used by the boarding party for collaborating in the Groove workspaces.

Figure 38. 6 dB omni 802.16 Antenna Onboard the Target Vessel

During the search phase, MSST discovered two radiation sources on board the vessel with the use of their Identifinders. Again, the spectrum files had to be uploaded from the Identifinders to the LLNL laptop, and from there via a flash memory stick to the boarding party Groove laptop for posting to the Boarding Party workspace in Groove. The events related to each one of them were:

- ***Source #1:*** It was discovered at 1226 in an exterior deck locker (Figure 39) and was reported via text message in Groove. A decision was made, not to open the locker door without verifying first the identity of the source. While the boarding party was working on posting the spectrum

files in Groove, a response came back from LLNL, which momentarily caused confusion to the boarding officer, since it did not concern source #1, but analysis of the radiation files sent previously by SFPD Marine Unit-3 RHIB. Furthermore, the two posted files in Groove, regarding source #1, were mislabeled (source named background and vice versa), which did not allow LLNL reachback to provide a correct analysis. As a result, a longer duration recording of the source spectrum was posted in Groove, in addition to a spectrum screen shot that had been requested by LLNL earlier. After receiving the new files, LLNL identified the source as Plutonium 239, although the response required further explanations, both to District 11 and the boarding officer. The LLNL response stated that the source "is not inconsistent with Plutonium 239," which caused uncertainty about three issues:

- Was that a case of WMD material or that source could be onboard a ship for other reasons? Was there a certain malevolent intent, or could it be authorized to be there?
- What were the implications of that discovery for the boarding party members and the San Francisco bay area?
- What was the level of certainty that it was Pu-239 and not something else?

Another issue that emerged after the initial radiation detection was the possibility that the locker was booby trapped, which prevented the MSST from opening its door. Although there was no evidence, it was something that needed further investigation. To complicate things further, the hazards to the boarding party from getting close to that source were unknown. Since there was not anything more to be done by MSST to provide certain answers about the situation, a decision was made by District 11, to anchor and secure the vessel and crew until DOE RAP arrived on scene and provided more reliable information.

Figure 39. Radiation Source #1 Onboard the Suspect Vessel (After: Bordetsky, 2006)

- ***Source #2:*** It was discovered at 1311 in the interior berthing compartment of the vessel. The radiation file that was posted in Groove, confused the LLNL reachback team because although it was suspected of being a smoke detector, the spectrum (neutron count) was not as expected. The initial suggestion of LLNL, was to send a RAP team equipped with germanium detectors, and afterwards it was requested to send photographs of the source. After the photographs from the digital camera were downloaded to the boarding officer's laptop and posted in Groove, it was determined that the abnormality of the source spectrum was due to its proximity to the source #1, and thus confirmed that it was, indeed, an old smoke detector.

In addition to the radiation search, the boarding party obtained fingerprint samples from the vessel's crewmembers. All three samples that were loaded onto the Biometrics Enrollment computer, returned a negative response (no match in the watch list) from the Biometrics Master computer in the TOC. Although the scenario dictated that the response should be a positive match, some issues in loading these samples onto the Biometrics Master computer did not allow for that to happen.

E. EXPERIMENT OUTCOMES - CONCLUSIONS

1. Network Performance

After the experience from past TNT MIO field trials, there were no problems with the network reliability and performance. The 802.16 link stretched up to the distance of 700 yards, although it could have been stretched even further (Figure 40). The directional antennas of 24 dB that were used initially, were replaced with omni ones of 6 dB, since

they required a continuous manual alignment between the TOC and the suspect vessel. At 600-700 yards, a stable Received Signal Strength Indicator (RSSI) of 80 dBm on average, was maintained in Redline's RF Link Monitoring tool (with the 6 dB antennas), to be disturbed only by random pitch and roll of the target vessel caused by wake from passing by ships. Overall, the 802.16 link had an ample performance, and was sufficient to accommodate the requirements of the exchanged data.

Figure 40. 802.16 Link between TOC and Suspect Vessel

As expected, the target vessel's navigation radar (Furuno, I-Band/9 GHz) did not affect at all the performance of both the 802.16 and the 900 MHz links. A minor issue that emerged was during the simultaneous connection of the boarding officer's laptop (Solar Winds) on both the 802.16 subnet via Ethernet and the ITT mesh via the wireless card interface. For unknown reasons, the wireless interface was being disabled randomly without any indication in the control panel / network connections. The problem was being solved by disabling and enabling again the interface through the control panel. Also, the

new AN-80's could not be used instead of the AN-50's, since one of them could not be configured, although that had been performed successfully in the previous TNT experimentation, two weeks ago in Camp Roberts.

The two subnets on board the suspect vessel (ITT mesh: 192.168.73.0, and 802.16: 192.168.72.0) included the following nodes and IP addresses, respectively:

Boarding Officer Laptop (Solar Winds)	192.168.72.128
	192.168.73.121
ITT Mesh Access Point – GPS receiver/poster (Target Vessel)	192.168.72.181
	192.168.73.1
Boarding Officer Laptop (Groove)	192.168.72.30
Biometrics Enrollment Laptop	192.168.72.10
Biometrics Master Laptop	192.168.72.11
Pelco Camera (Target Vessel's bridge view)	192.168.72.214
Pelco Camera (input from Target Vessel's monitoring cameras)	192.168.72.225
AN 50 Radio (TOC)	192.168.72.26
AN 50 Radio (Boarding Party)	192.168.72.25
Target Vessel laptop (used only on June 13)	192.168.72.129

Table 2. TNT 06-3 Extension to Sea Network: IP Addresses of 802.16 / ITT Subnet Nodes

The following figures from Solar Winds Network Monitoring Tool, illustrate the performance of the 802.16 link in terms of Response Time and Packet Loss, both for June 13 (Figure 41) and June 14 (Figure 42). Throughput is not possible to be monitored directly on Redline's AN-50's, since AN-50's MIB's are not yet compliant with Solar Winds. Both response time and subsequent packet loss remained low, both days of the field trial. Any major increase in these values can be attributed to misalignment of the antennas (at least on June 13, when the directional antenna had to be manually aimed towards the TOC). A useful tool to indicate the antenna misalignment was the RF Link Monitoring tool; any drop on RSSI/SNR values was followed by manual correction of the antenna aiming. The average response time was close to 5 ms, while the packet loss was nearly 0%. Correlation between the amount of the exchanged information (from Observer's Notepad and Groove's event log) and the response time / packet loss values did not indicate any connection between them. Thus, we can indirectly conclude that the provided throughput of the 802.16 link was more than enough.

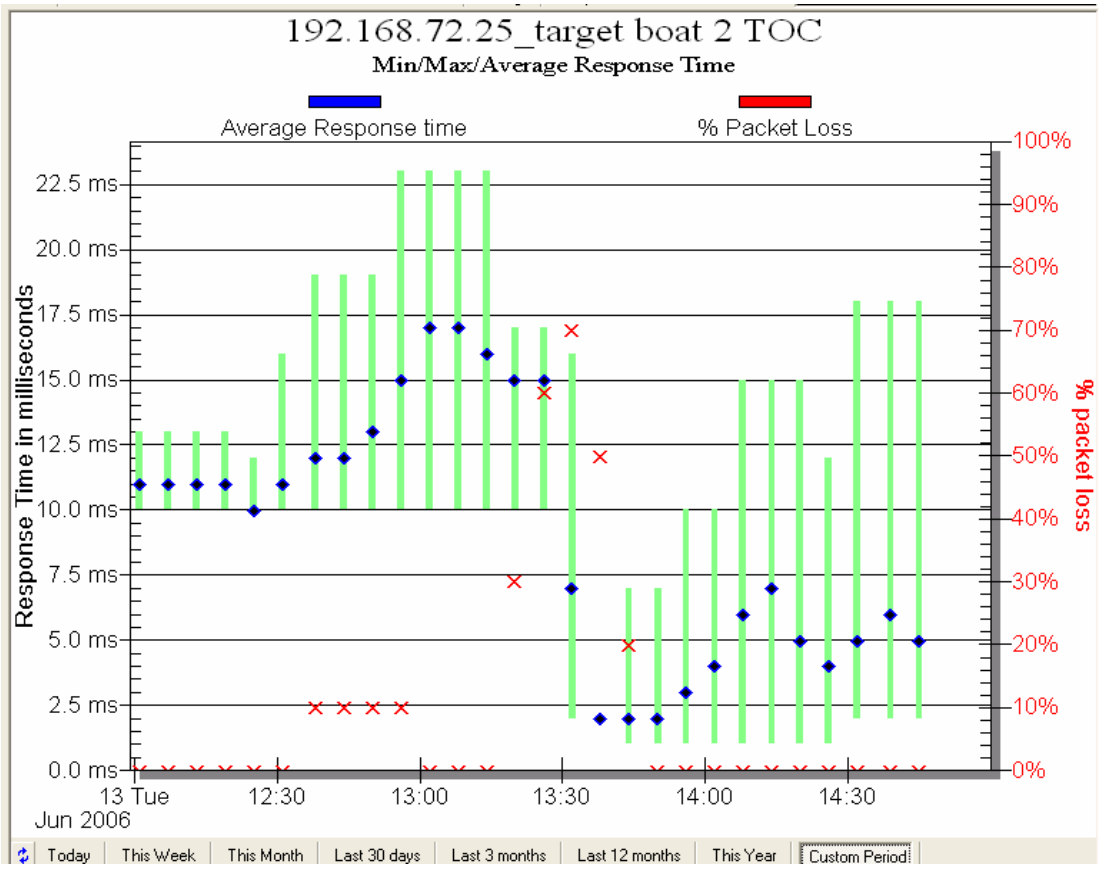

Figure 41. Response Time and Packet Loss of 802.16 Link (June 13)

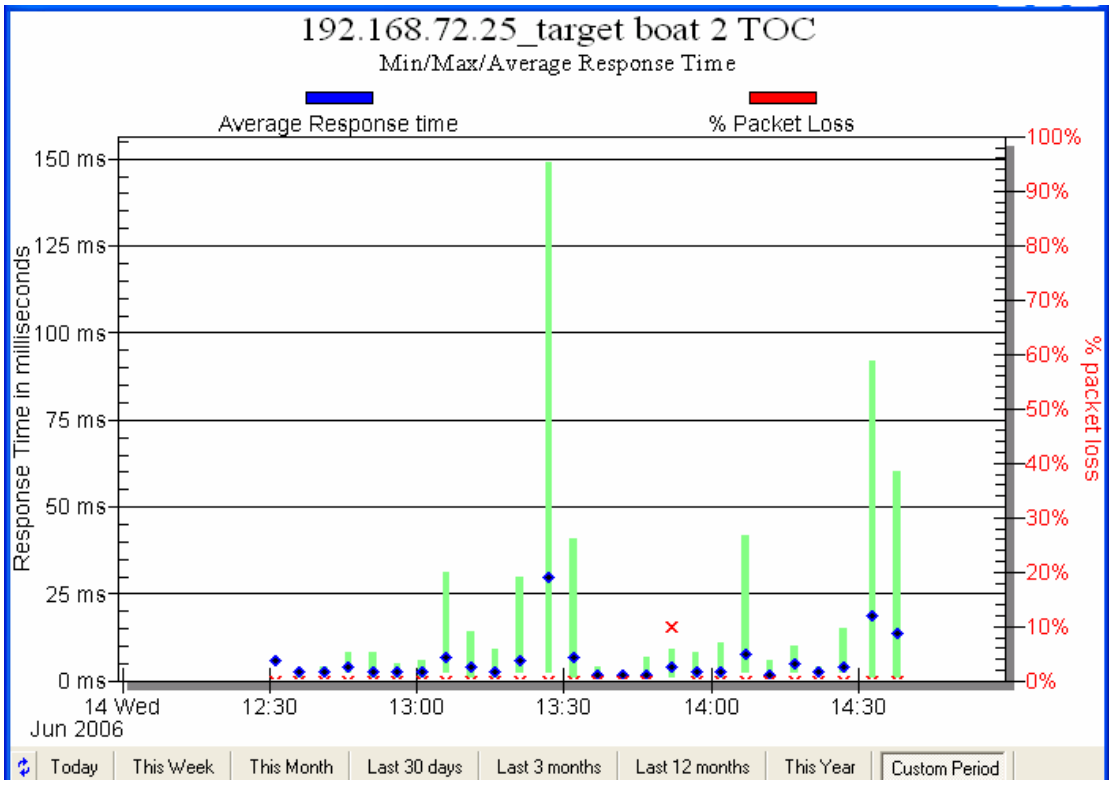

Figure 42. Response Time and Packet Loss of 802.16 Link (June 14)

Data from Solar Winds about other nodes indicate that everything went smoothly without any problem at all. The average bps from the boarding officer's laptop was approximately at 0.8 Mbps / 0.7 Mbps in/out, while the response time and the packet loss were negligible (Figures 43 and 44). Other nodes, such as the network monitoring laptop of boarding officer and the GPS receiver/poster laptop, also had negligible contribution to the total throughput of the 802.16 link (Figures 45 and 46). The total throughput of the link was estimated on the field trial of June 13 to be over 2 Mbps; the measurement was observed via Solar Winds bandwidth gauge on the boarding officer's laptop (Groove).

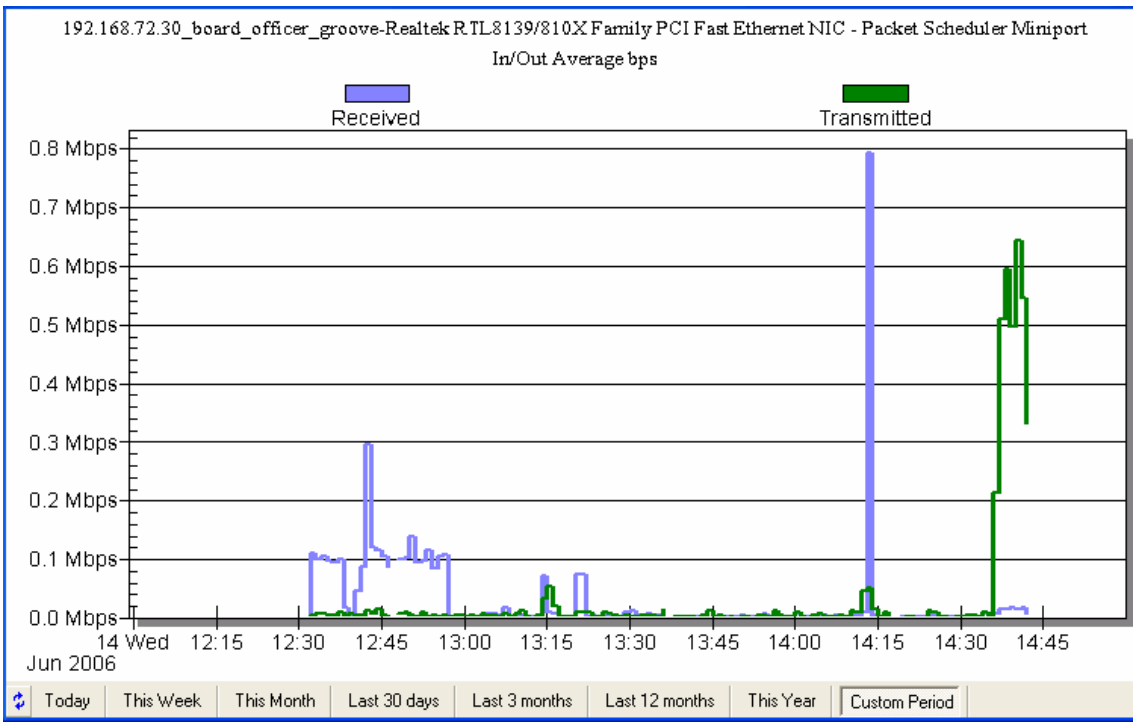

Figure 43. Boarding Officer's Laptop/Groove-In/Out Average bps (June 14)

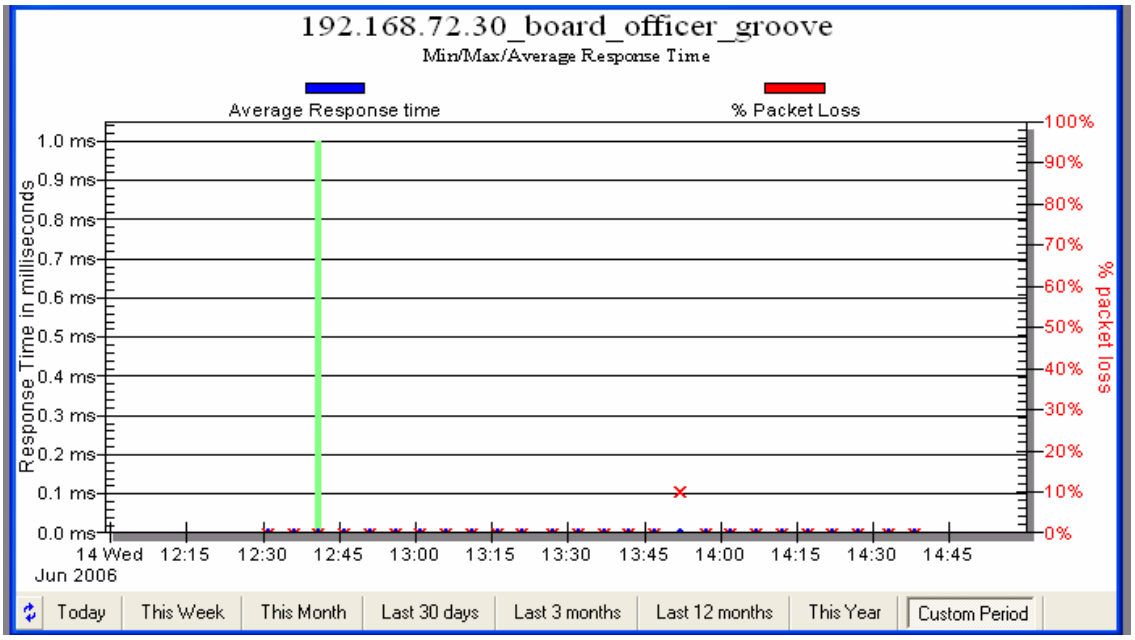

Figure 44. Boarding Officer's Laptop/Groove-Response Time and Packet Loss (June 14)

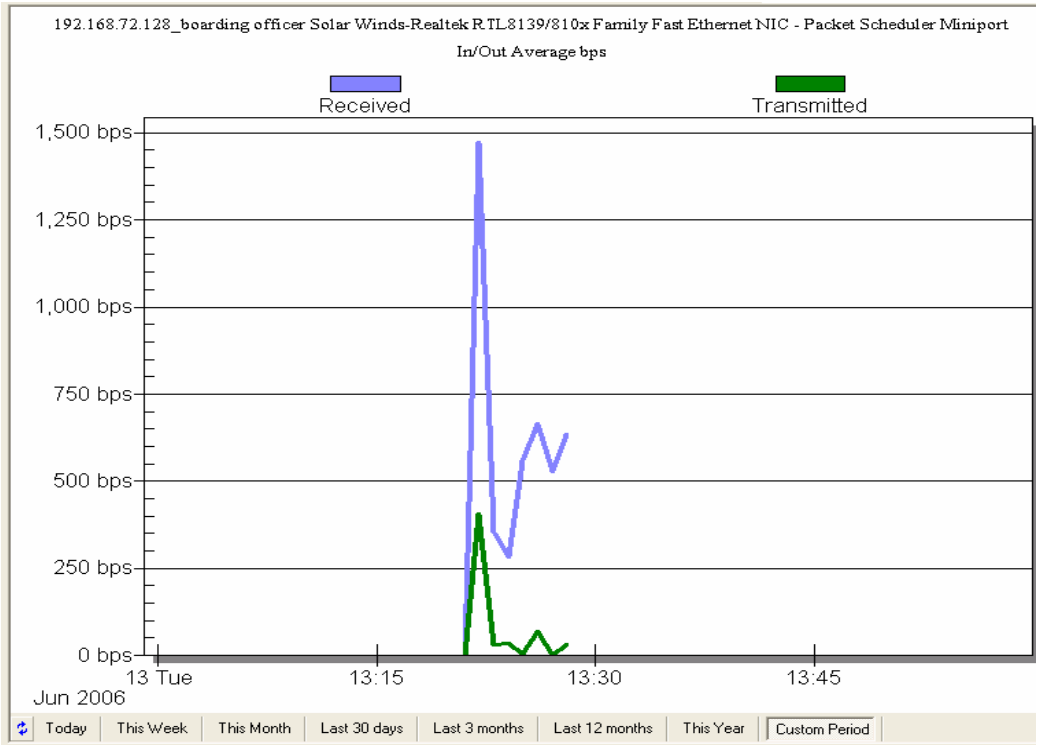

Figure 45. Boarding Officer Laptop (Solar Winds) - In/Out Average bps (June 13)

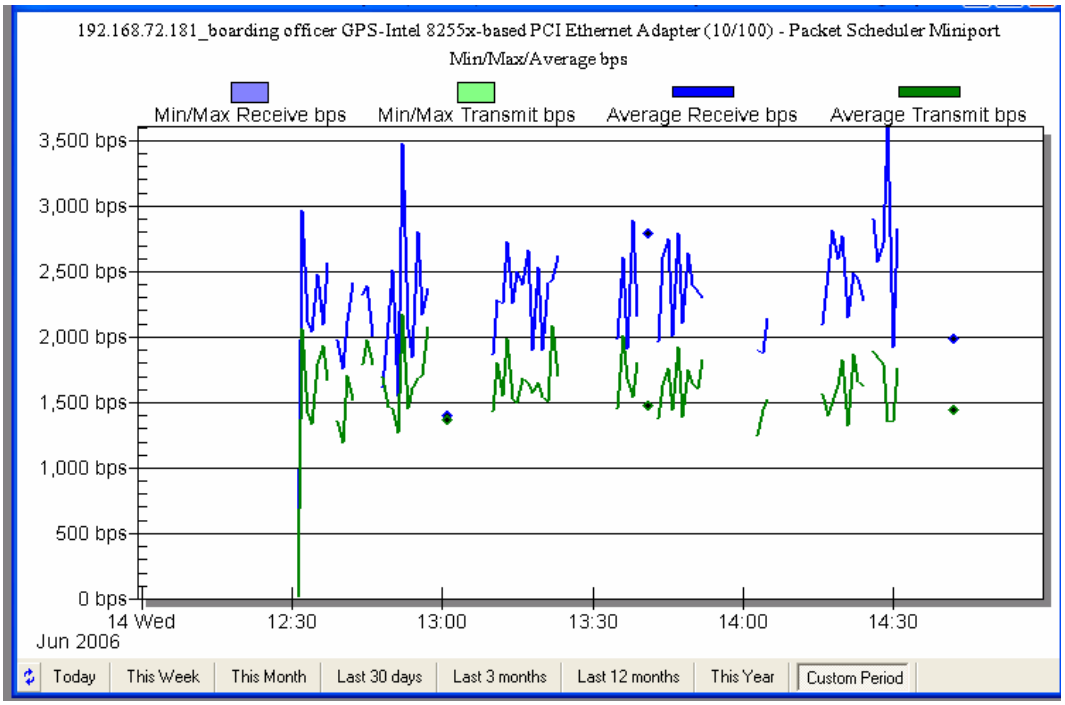

Figure 46. Boarding Officer Laptop (GPS Receiver / Poster) - In/Out Average bps (June 14)

2. Collaboration and Situational Awareness

As previously mentioned, the collaboration environment of TNT 06-3 was much more complex than the previous experiments, incorporating more players into the scene of action, greater exchange of information from different sources and through different collaborative tools, and thus increasing the reality level of the scenario. Over and above past TNT MIO field trials, the "fog and friction" was well applied in this one. There were some issues revealed, though, regarding the situational awareness of the key players and their level of successful collaboration.

First, files posted on Groove's workspaces did not follow standard naming procedures. Naming them properly, so that the recipients could easily understand what they contained, was up to the boarding party. As a result, additional information regarding the contents of these files had to be exchanged through Groove's chatting, causing delays in getting an analysis report from reachback. On one occasion, wrong labeling of the radiation spectrum files, caused wrong analysis of the findings by LLNL reachback. Had not that incident been identified early enough, it would have brought further implications on the decision making process. The possibility of such problems to occur increases as more data files from different sources are posted. A solution to that problem would be to adopt the rules and procedures followed in such cases by military operators. A ship tracking multiple radar contacts, for example, assigns a specific letter (contact type identification), followed by a unique track number (instance identification) to each contact, so that a report on a specific track (on both data and voice networks) cannot be confused with reports about other tracks. Therefore, adopting a standardized naming convention, in order to discriminate data of different types (photographs, spectrum or biometrics files) and track numbers for discriminating between the different instances of the same data type, would be more appropriate. Additionally, a time stamp added on each file label, would also accommodate the distinction between consecutive reports about the same instance of data.

Apart from the naming of the files, another issue concerning the comprehension of the exchanged information, was the language used in Groove's chat. Although all nodes of a network may use the same language, the semantics of words and phrases may differ. That is the reason for using a standardized language in military communications,

in order to cancel the ambiguity of people's different interpretation of the same piece of information. For example, the phrase "not inconsistent with plutonium" was interpreted in many different ways by the boarding party; as "high probability of being plutonium", or "plutonium cannot be excluded", which mean different things, and may be followed by different decisions and further actions. That issue is sure to deteriorate with the addition of international collaborators who have a native language other than English. Therefore, the language used in the collaboration environment needs to be standardized so that it does not become a barrier in the cognitive process.

The presence of LLNL personnel on board the target vessel helped in the comprehension of the incoming information from LLNL reachback regarding the analysis of the radiation spectrum files. It is neither possible nor necessary to give information to boarding party members that they cannot process due to their lack of education. Operators need simple information and so do decision makers on the tactical or operational level.

The use of multiple Groove workspaces was justified in order to separate the multiple domains of information that had to be exchanged between the boarding party and the rest of the nodes. As a result, the workload for the boarding party was increased, since the boarding officer was a client in all three of the workspaces; all of them had to be monitored and updated, while multiple pieces of information had to be replicated in each one of them quite often. Although the situational awareness of the boarding officer was increased regarding the findings on the target vessel, the command and control capabilities decreased since there was no time to monitor where each boarding party member was, or what else was happening on the ship. On the other hand, the use of multiple workspaces is inevitable; as the number of the Groove clients increases (which is necessary for making the concept of TNT MIO fully operational), the amount of the exchanged information will increase exponentially, in which case the "need to know" rule should be strictly enforced. A solution to that issue would be the addition of extra personnel in the boarding party, in order to respond to the additional flow of information.

Boarding operations have many aspects that require a broad range of expertise in order to deal with all of them. For example, the possibility of the first radiation source

being booby trapped would require assistance from EOD specialists. At the present, there are still more aspects to be covered (such as emergency medical assistance that finally was not able to be included at this field trial) and more experts to be included in the collaboration environment.

Overall, the situational awareness of all participants was sufficient to enhance the cognitive process and produce correct decisions, due to the participation of the right players in the collaboration environment and the use of Groove, SA and E-Wall collaboration tools. The addition of international players (Austria and Swedish authorities) proved that there are no limits on who is to be included in the collaboration. It no longer matters how far, but only who possesses the right information. Minor collaboration discrepancies that occurred were a valuable lesson in order to transform the boarding procedures, and align them with the new technology and tools available.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The main concept examined in this study was the extension of NCW to the front line war fighter, and specifically the members of a boarding team conducting Maritime Interdiction Operations. Throughout the TNT field experimentation performed in the San Francisco bay area by the NPS / CENETIX lab personnel, it was proven that innovative, leading edge technologies are about to make that concept reality; the focus now is on the transition of successfully implemented technology into full operational capability. Specifically, in this thesis we have examined:

- The applicability of the employed technologies on the operational needs of a MIO environment. How are concepts such as rapidly deployable OFDM, UWB, and adaptive, self healing, ad hoc networks most suitable for our purposes? What are the reasons for their selection, development and implementation, based on their distinctive features?
- How these technologies provide a common operating picture and enhance the situational awareness of the war fighter and the decision making capability of the operational commander
- Which operational requirements have been satisfied, and which are still pending for future consideration and experimentation

B. RECOMMENDATIONS FOR FUTURE RESEARCH

1. Increasing Range

So far, the range of the ship-to-ship or ship-to-shore 802.16 links is relatively short. This can be attributed to the high utilized frequency, the low output power, and the use of omni or low gain, wide lobe antennas. These three limiting factors could be addressed with the migration of the frequency to the lower and even the licensed range that provides better propagation characteristics, which in turn could diminish the limit on the maximum allowed output power. Furthermore, the acquisition of high gain, self aligning antennas would give the 802.16 links their real potentials in range and subsequently in throughput. Another possible remedy could be the use of fixed or mobile nodes acting as repeaters. UAV's, maritime buoys, manned or unmanned boats and land stations could be used for that purpose. The experience of the NPS/CENETIX lab team is already in place in the case of using UAV's in extending the range of the ship-to-ship or

the ship-to-shore 802.16 links. The issue in the use of UAV would then be, to minimize the weight and volume of the Redline's equipment (bridge, power supply, omni antenna) in order to match the payload requirements of the UAV, and also to increase the endurance of these UAV's in order to be able to sustain the entire boarding operation duration.

2. Increasing Portability

Although the use of Redline's AN-80 did not become possible during TNT 06-3 field trial, this should not be a problem for future experiments. Compared to the AN-50, AN-80's provide the same performance included in a lower volume and weight package. Further increases in portability could be achieved with standardization of the required equipment in ready to go packages, whether bergen rucksacks or pelican cases.

3. Expanding the Collaborative Environment

A lot of required information and knowledge is still unavailable to the boarding party. State organizations and centers of expertise, either civilian or military, are still to join the collaborative environment and enhance the present potentials of the MIO's.

4. Expanding the Operational Capabilities

Additional equipment could expand the operational capabilities of the boarding party in terms of night operations, and data collection. That kind of equipment includes video cameras with IR capabilities, allowing for searching vessels and sending video feedback during night time, and other biometric enrollment devices, such as facial recognition and voice identification devices.

5. Implementation of TNT MIO Network to Other Maritime Applications

MIO's are not the only application that requires broadband data connectivity and collaboration. Considering other maritime operations conducted by the Navy, we can find many other areas to apply the same network setup. For example, during MCM (Mine Counter Measure) operations, there are vessels operating in close ranges, plotting positions of mines or cleared corridors, and requiring exchanging data in order to produce and update a common minefield picture. In such a case, this would be possible with the use of the existing MIO network and by employing an application layer GIS (geographical information system).

LIST OF REFERENCES

Alberts, D., Garstka, J., Stein, F., (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised). DoD C4ISR Cooperative Research Program.

Bahai, A., Saltzberg, B., Ergen, M., (2004). *Multi-Carrier Digital Communications: Theory and Applications of OFDM.* Springer Science + Business Media Inc.

Bordetsky, A. (2006). *Email: Subject: More TNT Photos.* From*:* abordets@nps.edu.

CommsDesign. *Why Such Uproar over Ultrawideband?* http://www.commsdesign.com/design_corner/OEG20020301S0021, Last accessed April 16, 2006.

Digit-life. *Following the IDF: Ultra Wide Band Wireless Data Transfer Technology*. http://www.digit-life.com/articles2/uwb/index.html, Last accessed April 16, 2006.

Hayes-Roth, R., (2006). *Hyper-Beings: How Intelligent Organizations Attain Supremacy through Information Superiority*. Booklocker.com, Inc.

IEEE. *IEEE 802.16 Published Standards and Drafts.* http://www.ieee802.org/16/published.html, Last accessed May 4, 2006.

Intel. *Ultra-Wideband (UWB) Technology*. http://www.intel.com/technology/comms/uwb/, Last accessed April 16, 2006.

International Engineering Consortium. *OFDM for Mobile Data Communications***.** http://www.iec.org/online/tutorials/ofdm/topic04.html, Last accessed April 12, 2006.

Marakas, G. (2003). *Decision Support Systems in the 21st Century*. Prentice Hall.

Marvin, C., (2005). *802.16 OFDM Rapidly Deployed Network for Near-Real-time Collaboration of Expert Services in Maritime Security Operations*. Master's Thesis, Naval Postgraduate School, Monterey, California.

Naval Aviation Schools Command. *Situational Awareness (SA).* https://wwwnt.cnet.navy.mil/crm/crm/stand_mat/seven_skills/SA.asp, Last accessed July 26, 2006.

Nekoogar, F., (2006). *Ultra-Wideband Communications. Fundamentals and Applications.* Prentice Hall.

Network World. *IEEE 802.16 for Broadband Wireless***.** http://www.networkworld.com/news/tech/2001/0903tech.html, Last accessed April 18, 2006.

Ohrtman, F., (2005). *Implementing WiMAX Handbook. Building 802.16 Wireless Networks.* McGraw-Hill Companies, Inc.

Olexa, R., (2005). *Implementing 802.11, 802.16 and 802.20 Wireless Networks: Planning, Troubleshooting and Operations.* Oxford, UK: Newnes.

PaloWireless. *Ultra Wideband (UWB) Tutorials.* http://www.palowireless.com/uwb/tutorials.asp, Last accessed April 16, 2006.

Parrish, W., Tovar, D., (2005). *Tactical Wireless Networking in Coalition Environments: Implementing an IEEE 802.20 Wireless End-User Network Utilizing FLASH-OFDM to Provide a Secure Mobile Extension to Existing WAN.* Master's Thesis, Naval Postgraduate School, Monterey, California.

Prasad, R., (2004). *OFDM for Wireless Communications Systems.* Boston, London: Artech House Inc.

Redline Communications. 2005. *AN-50e Datasheet.* Available at http://www.redlinecommunications.com/news/resourcecenter/productinfo/an50e.pdf. Last accessed May 4, 2006.

Redline Communications. 2005. *Can WiMAX Address Your Applications?* White paper, available at http://www.redlinecommunications.com/news/resourcecenter/whitepapers/Can_WiMAX_Address_Your_Applications_final.pdf. Last accessed at May 4, 2006.

Smith, C., Meyer, J., (2005). *3G Wireless with WiMAX and WiFi: 802.16 and 802.11*. McGraw-Hill Companies, Inc.

Subramanian, M., (2000). *Network Management, Principles and Practice*. New York: Addison Wesley.

Suitor, K. 2004. *What WiMAX Forum Certified™ Products Will Bring to Wi-Fi™.* Business White Paper, Redline Communications. Available at www.redlinecommunications.com, Last accessed April 19, 2006.

Technische Universiteit Delft. *OFDM As a Possible Modulation Technique for Multimedia Applications in the Range of mm Waves.* http://www.ubicom.tudelft.nl/MMC/Docs/introOFDM.pdf, Last accessed April 13, 2006.

Walter, B., Gilster, R., (2002). *Wireless LANs End to End*. Hungry Minds, Inc.

Webopedia. *UWB***.** http://www.webopedia.com/TERM/U/UWB.html, Last accessed April 16, 2006.

Wikipedia. *Ultra Wideband***.** http://en.wikipedia.org/wiki/Ultra_wideband, Last accessed April 16, 2006.

Wikipedia. *WiMAX*. http://en.wikipedia.org/wiki/WiMAX, Last accessed May 4, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan Boger
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

4. Alexander Bordetsky
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

5. Eugene Bourakov
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

6. Embassy of Greece, Naval Attaché
   Washington DC

7. LCDR Georgios Stavroulakis
   Hellenic Navy General Staff
   Athens, Greece